Before the
Federal Trade Commission
Washington, D.C.

Complaint seeking investigation, enforcement, penalties, and other relief as appropriate against Facebook, Inc.	Submitted November 15, 2018

I. Introduction

1. On September 28, 2018, Facebook, Inc. announced that 50 million users had been compromised in a massive data breach that put their entire accounts in the hands of unknown rogue actors. An additional 40 million users also had their accounts reset due to uncertainty about the scope of the breach.

2. While Facebook, Inc. has released few details about the attack, it is clear that virtually all the information users provided to Facebook, Inc. was potentially exposed, including personal biographical data, private messages, photographs (including those uploaded but not shared), and credit card numbers. Once inside Facebook's security wall, the attackers stood in users' shoes – with complete and total control over their profiles, accounts, and social media interactions.

3. The attackers also gained access to any apps or services that the victims had linked to their Facebook account using the corporation's "Facebook Login" feature. This put Facebook-connected users of apps like Tinder, Bumble, Spotify, Uber and thousands more at risk of having their accounts hijacked and misused.

4. This breach is the latest in a long string of Facebook, Inc. privacy violations. In 2007, the company apologized for sharing private information with user friends without asking permission. In 2011, the company made false claims that users would retain meaningful control over their privacy, leading to a landmark 2011 Consent Decree with this agency. In 2013, a bug exposed emails and phone numbers. This bug

was related to uploads of user contact lists. In 2017, the massive Cambridge Analytica scandal allowed the data of 87 million user profiles to be downloaded off the platform and used to manipulate the 2016 US Presidential election and Brexit referendum.

5. The breach also comes just a few months after Facebook, Inc.'s CEO Mark Zuckerberg told the United States Congress that "we have a responsibility to not just build tools, but to make sure those tools are used for good . . . . It will take some time to work through all of the changes we need to make, but I'm committed to getting it right."

6. Facebook, Inc. has a track record of prioritizing advertising over security. In October, 2018, academics uncovered the company was using contact information handed over for security purposes, such as for two-factor identification logins or or in order to receive alerts about new log-ins to a user's account, to engage in ad targeting. The surveillance-intensive business model of targeted advertising combined with the need to secure data presents perhaps an unresolvable conflict of interest for the company as currently constituted.

7. Facebook, Inc. is a serial privacy violator that cannot be trusted. It has grown too big and its products have become too integrated and too complex to manage. Not only can we no longer trust Facebook, Inc. to manage its system safely, the corporation no longer has the capacity to do so effectively.

8. The organizations filing this Complaint seek a thorough investigation of the "View As" breach and appropriate enforcement using all available remedies against Facebook, Inc. for its apparent breaches of the FTC Act and the 2011 Consent Decree.

9. The organizations filing this Complaint also call for a broader investigation into a far more fundamental question – has Facebook, Inc. grown so large and complex that it is no longer governable at all?

II. The Freedom from Facebook Coalition

10. The Freedom from Facebook Coalition brings together diverse, non-partisan organizations representing consumers, workers, policy experts, creative artists and ordinary citizens from all walks of life demanding strong enforcement of consumer protection laws and a healthier, more open and transparent and competitive digital economy.

11. Our members include: Open Markets Institute, Citizens Against Monopoly, the Communications Workers of America, the Content Creators Coalition, Democracy for America, Demand Progress, Jewish Voters for Peace, Move On, MPower Change, Public Citizen, RootsAction, and Sum of Us.

III. Facebook, Inc.

12. Facebook, Inc., a Delaware corporation with its operational headquarters in Menlo Park, California, was founded in 2004 in Cambridge, Massachusetts by Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, Andrew McCollum, and Chris Hughes. Facebook, Inc. owns three significant social networks: Facebook, Instagram, and WhatsApp.

13. Facebook, owned by Facebook Inc., is the largest social media network in the world with over 2 billion daily active users globally, including 214 million daily users in the United States alone. Every day its users post 55 million status updates, upload 350 million photographs, 'like' nearly 6 billion posts, and send 60 billion messages over its proprietary Messenger network. Its apps are downloaded 1.06 million times a day, and the corporation gains 400 new users every minute.

14. Much of Facebook Inc.'s growth has been fueled by mergers and acquisitions that expanded the corporation's product offerings while taking potential competitors off the field. These include the acquisition of Instagram in 2012 and the acquisitions of WhatsApp and Oculus VR in 2014. As far as we are aware, no proposed Facebook, Inc. acquisition has ever been blocked by a US regulatory authority.

15. Facebook, Inc. is currently one of the most valuable companies in the world. Fortune Magazine lists it as the 76th largest corporation in the United States by revenue, and it has a market value at the time of this filing of $406.41 billion *(as of Nov. 15, 2018)*].In the second quarter of 2018, the most recent for which data is available, it earned revenue of $13.23 billion, or $143.8 million a day.

16. The bulk of Facebook, Inc.'s revenue comes from advertising targeted at its users using data the corporation collects from multiple channels, including information users share with its social networking

subsidiaries and data it captures by tracking and surveilling user activities across the web.

17. Facebook, Inc.'s ability to mine user data and target ads is uniquely robust in the US economy, due to the corporation's extraordinary scale, the personal nature of information its users share, and the breadth of its related products and services including Instagram, WhatsApp, Messenger. Only Google has comparable scale and reach, though even Google cannot match the depth of Facebook, Inc.'s social networking data.

18. Facebook, Inc.'s data reach is further extended by its "Facebook Login" product that allows user to sign up for other apps and websites based on their Facebook credentials and without creating a new, freestanding account. Facebook captures two-thirds of the social logins for sites that use this kind of external credentialing, giving it a rich new source of data about user activities at tens of thousands of non-Facebook websites.

IV. Facebook's Repeated Breaches of its Users' Privacy and Data Security

19. The 2006 launch of Facebook's "news feed" automatically broadcast a host of user activities and updates to all their friends as a default feature without clear disclosure or consent. Mark Zuckerberg admitted at the time that "We really messed this one up" and that the corporation "didn't build in the proper privacy controls right away".

20. Facebook's Beacon advertising system, launched in 2007, tracked users' activity on third-party partner sites back to Facebook and automatically posted them to user profiles, even when users weren't logged in to Facebook and despite user efforts to opt out of the program. Facebook, Inc. ultimately paid $9.5 million to settle these claims.

21. In 2010, a Harvard Professor filed a complaint with this agency revealing that Facebook was sharing user information with advertisers including profile details and web activity without disclosure and consent.

22. In November 2011, the FTC entered into a far ranging consent decree with this agency, arising out of repeated breaches of user privacy and false claims that Facebook, Inc. would protect user information. The

charges grew out of a December 2009 change to the Facebook website that made users' private information public without their consent, and repeated Facebook, Inc. misrepresentations about the information it shared with third party apps, the it shared with advertisers, and the handling of data after user deleted or deactivated their accounts.

23. In 2011, Facebook incorporated facial recognition as a default setting on its 'tag suggestions' feature without clear disclosure or obtaining consent from users for this invasive new technology. After consumer outcry, Facebook, Inc. admitted "we should have been more clear with people during the roll-out process when this became available to them".

24. In January 2012, Facebook launched a secret experiment to manipulate user moods by feeding nearly 700,000 test subjects skewed diets of positive or negative news, without any disclosure or consent. The privacy watchdog EPIC filed a complaint with this agency about this unethical "research" study.

25. In 2013, a bug made the emails and phone numbers of 6 million Facebook users public to users who had some tangential connection to them on the site (ie. 'friends of friends'), despite that information being designated 'private' or for 'friends only'. This breach was not noticed by Facebook, Inc. but only came to light after a "white hat" hacker uncovered and reported it.

26. In what should have been a wakeup call ahead of the Cambridge Analytica, a software engineer was able to automatically scrape or harvest names, profile photos, and locations of users by entering their mobile phone numbers into the platform's "Who can find me?" feature, even if the phone numbers were set to private. By generating random phone numbers, he was able to collect data on thousands of users.

27. In 2018, it was revealed that the data of 87 million Facebook users was shared with political consulting firm Cambridge Analytica. 270,000 users took a quiz designed by Cambridge Analytica to extract users' profile information and in the process, exposed the profile information of their entire "friends' list". Cambridge Analytica proceeded to sell this data, via their consulting services, to various parties, including the 2016 Trump presidential campaign and the Brexit "leave" campaign.

28. Facebook has used phone numbers provided by users for two-factor authentication security purposes in order to target advertisements, a use they did not clearly disclose, explain, or obtain separate consent for. This follows an earlier scandal in which the corporation spammed users' two-factor authentication number with texts and then automatically posted their replies to that spam as status updates for all to see.

29. In the spring of 2018, Android users realized Facebook was using its Messenger app to track and log their texts and phone calls. Facebook, Inc. claimed users granted Facebook permission to do this when they synced their phone contacts list with the Facebook Messenger app.

30. On October 11, 2018, Facebook suspended the Russian firm SocialDataHub "because they were scraping people's data" from the site.

V. Facebook's Many Promises to Protect Users' Privacy and Keep Their Data Secure

31. Since its inception, Facebook, Inc. and Mark Zuckerberg have promised users that their data is protected, and they have complete control over their privacy on the platform.

32. In 2005, Mr. Zuckerberg said of the platform, "We're not forcing anyone to publicize any information about themselves. We give people pretty good control over their privacy. I mean you can make it so that no one can see anything, or no one can see your profile unless they're your friend."

33. A decade later, Mr. Zuckerberg responded to the NSA PRISM program's collection and use of Facebook data, writing in a personal post, "To keep the internet strong, we need to keep it secure. That's why at Facebook we spend a lot of our energy making our services and the whole internet safer and more secure. We encrypt communications, we use secure protocols for traffic, we encourage people to use multiple factors for authentication and we go out of our way to help fix issues we find in other people's services."

34. Facebook, Inc. and Mr. Zuckerberg continue to promise data security to users, even as that data is repeatedly compromised. After the Cambridge Analytica scandal, Zuckerberg wrote, "We have a

responsibility to protect your data, and if we can't then we don't deserve to serve you. I've been working to understand exactly what happened and how to make sure this doesn't happen again… We will learn from this experience to secure our platform further and make our community safer for everyone going forwar

35. In a full-page newspaper ad purchased and placed around the same time, Mr. Zuckerberg again promised to more completely protect users' data: "This was a breach of trust, and I'm sorry we didn't do more at the time. We're now taking steps to make sure this doesn't happen again. . . I promise to do better for you."

36. In April of this year, Mr. Zuckerberg testified before the Senate Judiciary Committee, emphasizing the responsibility of Facebook's developers to protect user data and once again stating the corporation was committed to stopping such breaches: "It's not enough to give people control of their information, we have to make sure developers they've given it to are protecting it too. Across the board, we have a responsibility to not just build tools, but to make sure those tools are used for good. It will take some time to work through all of the changes we need to make, but I'm committed to getting it right."

37. However, influential voices in tech including former Facebook insiders have questioned these statements and commitments

38. After selling his corporation, WhatsApp, to Facebook, Inc. 2014 and subsequently leaving the corporation a few years later, Brian Acton told *Forbes*, "I sold my users' privacy. I made a choice and a compromise. And I live with that every day."

39. Chris Hughes, a co-founder of Facebook, Inc. who left the corporation in 2007, said in response to the Cambridge Analytica scandal, "The idea that this was unforeseeable seems like a stretch. The public reckoning now is very much overdue."

40. Apple CEO Tim Cook, differentiating Apple from Facebook, Inc., warned about the platform: "[Apple has] never believed that these detailed profiles of people, that have incredibly deep personal information that is patched together from several sources, should exist. [These profiles] can be abused against our democracy. It can be abused by advertisers as well."

41. Roger McNamee, an early investor in Facebook, Inc., has spoken out at length about what the platform has become, arguing that Facebook has "behaved irresponsibly in the pursuit of massive profits" and has "consciously combined persuasive techniques developed by propagandists in the gambling industry with technology in ways that threaten public health and democracy."

42. McNamee has warned about the risk of using Facebook, Inc. to user privacy, telling CNBC, "There's been an increasing understanding that when you're using Facebook, a lot of bad things are going to happen to you, as a user. That is not a 100 percent guarantee, but the risk is really, really high."

VI. The 2018 Breach of Facebook's "View As" Feature

43. On September 28, 2018, Facebook, Inc. disclosed a major security breach that had potentially affected nearly 50 million user accounts. On October 12, the company clarified that 30 million accounts appear to have been actually compromised.

44. By exploiting a vulnerability in Facebook's "View As" feature – which allows users to see how their profiles appear to others – hackers were able to harvest highly sensitive "access tokens" that could then be used, in Facebook's words, to "take over" accounts. Facebook, Inc. describes these access tokens as "digital keys" that would let hackers pose as the user online, engage with their friends and contacts, and use or share any of their information, including private messages, pictures that had been uploaded but not shared, and payment methods.

45. In addition, because these access tokens are used to verify "Facebook Login" requests, the hackers could also access and use any linked app or third-party service, including dating sites, health portals, and message boards.

46. The potential harms of this kind of data breach go well beyond the ordinary damage caused by compromise of sensitive information. In our connected culture, being impersonated online is a deeply personal invasion that could run from the merely embarrassing – like having an unflattering photo shared – to the devastating – including lost friendships or broken relationships. The Ashley Madison breach – a

severe breach but one that did not raise the even more invasive specter of online impersonation – resulted in suicides, divorces, and job losses.

47. At this point, the toll of the Facebook "View As" breach is not known. Facebook, Inc. CEO Mark Zuckerberg stated on September 28 that "We do not yet know whether these accounts were misused." Several days later, the corporation reported it had "so far" found no evidence the access tokens were used to breach third party apps. On October 12, it revealed that extensive personal information had been breached along with access tokens, including "surname, gender, locale/language, relationship status, religion, hometown, self-reported current city, birthdate, device types used to access Facebook, education, work, the last 10 places they checked into or were tagged in, website, people or Pages they follow, and the 15 most recent searches."

48. FTC action is needed to ensure that Facebook, Inc. cannot sweep this matter under the rug with such vague and incomplete assurances. It is the only way to ensure victims of this breach have accurate information about what happened to them.

49. While European investigators have opened up their own review of this matter, it is vital for US enforcers to act as well. Facebook, Inc. is an American corporation and many US citizens were undoubtedly victims of this breach. The FTC has jurisdiction and a responsibility to protect US consumers and to set standards for the US-driven internet economy.

VII. Claims

50. The Freedom from Facebook Coalition asks the Commission to investigate and act on the following specific claims as well as any other potential violations of the FTC Act and all other authorities under its jurisdiction.

Claim 1
Breach of 2011 Consent Decree

51. In 2011, Facebook, Inc.'s violation of user privacy led them to settle with the FTC and agree to the terms of the Consent Decree finalized in 2012.

52. Under the agreement, Facebook, Inc. cannot misrepresent the privacy or security of users' personal information and is required, among other

things, to obtain affirmative consent to privacy changes, "establish and maintain a comprehensive privacy program designed to address privacy risks associated" with the operation and development of the site and related products.

53. The latest breach was the result of several errors in Facebook's "View As" feature's code, made when Facebook updated their video uploader in July 2017 – more than a year before the breach was discovered.

54. User data was exposed for 14 months, because Facebook, Inc. failed to "maintain a comprehensive privacy program" as promised in the consent decree and as promised by the corporation and Mark Zuckerberg as detailed in paragraphs 30-34 above.

55. Furthermore, Facebook, Inc. failed to inform users that system updates may compromise their data and implemented these flawed new features without the express consent of users.

56. The penalty, outlined in the consent decree, is $41,484 per user per day. This violation affected 50 million users for nearly 430 days, calling for trillions of dollars in potential fines.

Claim 2
Breach of Section 5 of the FTC Act

57. Section 5(a) of the FTC Act prohibits "unfair" or "deceptive" acts in interstate commerce.

58. Past FTC investigations including the Ashley Madison case and the LabMD case have made clear that lax data security practices can constitute unfair business practices under the FTC Act.

59. In this case, given the gravity of the risk of loss of control of accounts due to theft of access tokens, Facebook, Inc.'s failure to prevent the "View As" breach constitutes an unfair practice that violates Section 5(a).

60. Past FTC cases including the Uber case establish that misrepresentations or omissions regarding data security and privacy and failing to live up to promises made regarding the security of customer information constitute deceptive acts under the FTC Act.

61. In this case, in light of the severe "View As" breach, Facebook, Inc.'s many promises to take appropriate security measures regarding customer information, outlined in paragraphs 30-34 above, and its assurances regarding the safety and security of the "Facebook Login" feature constitute deceptive acts or practices that violate Section 5(a).

Claim 3
Call for Expanded Investigation and Report on Facebook's Privacy Abuses, Monopoly Power and "Ungovernability" under Section 6(b) of the FTC Act

62. The "View As" breach raises issues that go beyond Facebook's violation of the 2012 Consent Decree and its breaches of the FTC Act.

63. Accordingly, we call for an investigation pursuant to Section 6(b) of the FTC Act of the role of Facebook, Inc.'s market power in the internet ecosystem and the unique threats to consumers posed by its massive accumulation of data – including that supplied by users, that harvested by surveilling their activities online, and that obtained from other sources such as data brokers or corporate acquisitions.

64. This investigation should cover Facebook's use of "Facebook Login" to expand its data holdings and neuter potential competitors.

65. This investigation should review the impact of acquisitions such as WhatsApp and Instagram on the health of the social media market and the failure of meaningful alternatives to Facebook, Inc. to arise.

66. Most fundamentally, this investigation should consider the unique issues raised when corporations become as large and complex as Facebook.

67. Facebook, Inc.'s scale renders it unable to effectively manage risk within its operations. It cannot meaningfully moderate content or protect users from harassment and abuse. It is unable to keep its own promises or accurately determine whether it is adhering to commitments it has made to users, business partners, and regulators. It has become so complex and deeply intertwined with other platforms, apps, and services that no executive or engineer can responsible anticipate or evaluate the real-world consequences of policy changes or product revisions.

68. In our view, Facebook, Inc. at this scale cannot be governed in a coherent or safe fashion – one that no one could manage and that no amount of AI or clever engineering will ever successfully control.

69. The result is a corporation managed by apology. One where unfair and deceptive practices are baked into the business model – and forced upon locked-in consumers who have no alternatives in the market and no real choices but those that Facebook, Inc. gives them.

Claim 4
Request for Any Other Appropriate Enforcement Under Any Applicable FTC Authorities

70. We ask the FTC and its professional staff to additionally conduct its own independent evaluation of the legal and marketplace implications of the "View As" breach in the context of Facebook's repeated broken promises and privacy abuses and to take any additional investigative or enforcement steps that are available to it and warranted under the circumstances to protect consumers and address the harms caused by Facebook.

VIII. Remedies

71. We urge the FTC to seek maximum civil penalties for the breach of its 2012 Final Consent Order by Facebook, Inc. as well as permanent injunctive relief, restitution, the refund of monies paid, disgorgement of ill-gotten monies, and other any other appropriate relief related to Facebook's violations of the FTC Act and any other laws or requirements within the agency's jurisdiction.

72. These remedies should include specific consideration of breaking up Facebook, Inc., and separating its advertising and social networking businesses or its discrete platforms in order to resolve the inherent conflict in running a data-based advertising businesses while being responsible for vast amounts of personal customer information and to address the poor privacy incentives created when a company holds a data-derived monopoly and has no meaningful competition.

IX. Conclusion

73. The FTC is at a landmark moment. Facebook, Inc. and the other biggest tech platform monopolies are fast breaking all traditional bounds of size

and behavior. Consumers as a result look to you for meaningful protection and enforcement – especially in the case of a serial privacy violator like Facebook that already has one outstanding consent decree under your jurisdiction. A healthy internet economy requires consumers to have basic trust and confidence in the corporations they deal with – and that in turn requires strong and steady enforcement of the basic rules of the road. In these circumstance, for the benefit of consumers, fair competition, and the internet economy itself, the Freedom From Facebook Coalition urges you to take strongest possible action.

Respectfully submitted,

_Freedom From Facebook_____

Citizens Against Monopoly

Communication Workers of America

Content Creators Coalition

Democracy For America

Demand Progress

Jewish Voice for Peace

Move On

MPower Change

Open Markets Institute

Public Citizen

Roots Action

Sum Of Us

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

July 13, 2018

Joseph J. Simons, Chairman
Maureen K. Ohlhausen, Commissioner
Noah Joshua Phillips, Commissioner
Rohit Chopra, Commissioner
Rebecca Kelly Slaughter, Commissioner
Federal Trade Commission, Commissioner
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear FTC Chairman Simons and Commissioners:

We write to ask you to stop the transfer of user data from Facebook to Social Science One, pending a determination as to whether the transfer is permitted under the 2011 Consent Order. EPIC has sent detailed letter (enclosed) to the co-chairs of Social Science One explaining why the proposed study of Facebook users should be suspended as it violates both the Consent Order and the GDPR.

The Consent Order is clear: Facebook must obtain affirmative express consent before disclosing personal data to third parties.[1] As the FTC explained, Facebook must "obtain consumers' affirmative express consent before enacting changes that override their privacy preferences."[2] By transferring personal information to third-party researchers without (1) providing clear and prominent notice and (2) obtaining the affirmative express consent of users, Facebook will violate the 2011 Consent Order with the FTC. There is no exception for third-party research.

Facebook users have expressed great concern about third-party access to their data following the Cambridge Analytica scandal. This week the UK Information Commission Office issued an extensive report, fined Facebook, and warned specifically about the use of personal data "for purposes it was not intended for or that data subjects would not have reasonably expected."

We urge the FTC to advise Social Science One and Facebook that the data transfer may not occur until the Commission has completed its review regarding compliance with the Consent Order.

Respectfully,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Christine Bannan*
Christine Bannan
EPIC Administrative Law and Policy Fellow

[1] Fed. Trade Comm'n., *In re Facebook*, Decision and Order, FTC File No. 092 3184 (Jul. 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.
[2] Fed. Trade Comm'n, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, Press Release (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

BY EMAIL <media@socialscience.one>[1]

July 12, 2018

Professor Gary King
Professor Nathaniel Persily
Social Science One

Dear Professor King and Professor Persily,

We write to you, as co-chairs of Social Science One, to urge you to immediately suspend the data analysis activities announced this week,[2] pending a thorough and independent investigation of the privacy protections for Facebook users. For multiple reasons set out below, including the fact that the program does not comply with the GDPR and violates Facebook's 2011 consent order with the Federal Trade Commission, we do not believe the project may go forward.

While we respect the efforts to develop a new model for industry-academic partnerships, frankly you could not have picked a more controversial data set to launch this initiative. The third-party use of Facebook data has been the focus of substantial Congressional hearings, hearings in the European Parliament, and an extensive inquiry in the UK.[3] The recent report of the UK Information Commissioner's Office had this to say about the transfer of Facebook user data to research institutions: "Based on evidence we have in our possession, we are concerned about the way in which data was accessed from the Facebook platform and used for purposes it was not intended for or that data subjects would not have reasonably expected."[4] We recognize the opportunity provided by new privacy-preserving techniques to permit research access to very large data sets,[5] but again you have chosen the most controversial data set to test these methods.

---

[1] It is notable that no contact information is provided for any individual at the Social Science One website, nor is there any indication that a person has been designated by Social Science One to assess the privacy ramifications of the project.

[2] Social Science One, *Independent Research Commission Partnering with Facebook and 7 Nonprofit Foundations to Study Role of Social Media in Elections and Democracy Reveals New Name and Announces First Data Set is Available for Academic Research* (July 11, 2018), https://socialscience.one/blog/social-science-one-public-launch

[3] EPIC, In re Facebook (Cambridge Analytica), https://epic.org/privacy/facebook/cambridge-analytica/.

[4] Information Commissioner's Office, *Investigation Into the Use of Data Analytics In Political Campaigns*, (Jul. 10, 2018) at 22, https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf.

[5] *See* National Academies of Sciences, Engineering, and Medicine; Division of Behavioral and Social Sciences and Education; Committee on National Statistics; *Panel on Improving Federal Statistics for Policy and Social Science Research Using Multiple Data Sources and State-of-the-Art Estimation Methods*; Harris-Kojetin BA, Groves RM, editors. Federal Statistics, Multiple Data Sources, and Privacy Protection: Next Steps. Washington (DC): National Academies Press (US); 2017 Oct 2. Available from: https://www.ncbi.nlm.nih.gov/books/NBK475779/ doi: 10.17226/24893

Social Science One describes the Facebook data as "the largest and most comprehensive information base ever used to study social media, and even some of the most extensive data ever used to study human behavior in general."[6] It is therefore of the utmost importance that you abide by all legal and ethical obligations related to the privacy rights of Facebook users.

I. Facebook Users Have Not Provided Meaningful Consent for the Collection and Use of Their Data

EPIC fully supports academic research on the effects of social media on democracy and elections. In fact, EPIC launched a project a year ago dedicated to safeguarding democratic institutions from foreign interference.[7] EPIC is presently engaged in several matters seeking information about Russian interference in the 2016 U.S. presidential election.[8] It is ironic and deeply troubling, however, that this research project involves violating the privacy of Facebook users' for the purpose of learning how social media influences elections. It was this very type of massive data collection by political firms such as Cambridge Analytica that raised alarms about the influence of social media on elections in the first place. In fact, the data obtained by Cambridge Analytica was originally collected for the purpose of academic research.

That is why the lack of meaningful consent from users necessitates suspending this study. Informed consent of human subjects is a basic ethical obligation for researchers, but one that Facebook and Social Science One have ignored. Facebook users will have no say over whether their personal data is used for this study. Facebook will not provide user with any mechanism to affirmatively opt-in to the use of their data. Neither Facebook nor Social Science One have indicated that Facebook users will even be provided with any information regarding the use of their data for this study. There is no indication that Facebook users will have the ability to opt-out if they do not wish to have their data used for research purposes. Facebook states that "[f]undamental to this entire effort is ensuring that people's information is secure and kept private."[9] But Facebook cannot claim to be respecting the privacy of its users if it fails to give users any control over whether their personal data is collected and used for this study.

II. The Transfer of Data Violates the FTC's 2011 Consent Order with Facebook

---

[6] https://socialscience.one/our-facebook-partnership

[7] EPIC, DEMOCRACY AND CYBERSECURITY: PRESERVING DEMOCRATIC INSTITUTIONS, https://www.epic.org/democracy/.

[8] *See*, EPIC v. FBI, https://www.epic.org/foia/fbi/russian-hacking/ (seeking records related to the FBI's response to foreign cyber attacks on democratic institutions in the United States prior to the 2016 Presidential Election); EPIC v. ODNI, https://www.epic.org/foia/odni/russian-hacking/ (seeking release of the Complete ODNI Assessment of the Russian interference with 2016 U.S. Presidential Election).

[9] Elliot Schrage and David Ginsberg, *Facebook Launches New Initiative to Help Scholars Assess Social Media's Impact on Elections*, Facebook Newsroom (Apr. 9, 2018), https://newsroom.fb.com/news/2018/04/new-elections-initiative/.

The FTC's 2011 Consent Order with Facebook is clear: Facebook must obtain affirmative express consent before disclosing personal information to third parties.[10] The Consent Order states that Facebook shall, prior to disclosing any information to third parties beyond the restrictions imposed by the user's privacy settings:

> Clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and **obtain the user's express consent**."[11]

As the FTC explained, this is a requirement that Facebook "obtain consumers' affirmative express consent before enacting changes that override their privacy preferences."[12] It is not enough for Facebook to bury a notice in its privacy policy – in addition to obtaining a user's affirmative consent Facebook must provide users with a clear and prominent disclosure that includes the identity of the third parties to whom the personal information will be transferred.

By transferring personal information to third-party researchers without (1) providing clear and prominent notice and (2) obtaining the affirmative express consent of users, Facebook will in clear violation of the 2011 Consent Order with the FTC. The *Wall Street Journal* has reported that outside researchers will have "the same access that employees would have" to user data.

The 2011 Consent Order was the result of Facebook's significant privacy violations, which EPIC documented in detailed complaints to the FTC in 2009 and 2010.[13] Chief among them was Facebook's practice of making non-public information available to third parties without users' knowledge or consent.[14] As we stated in 2009:

> Facebook's changes to users' privacy settings disclose personal information to the public that was previously restricted. Facebook's changes to users' privacy settings also disclose personal information to third parties that was previously not available.[15]

Earlier this year, Facebook was found to have allowed the political data mining firm Cambridge Analytica to obtain the personal information on 87 million users, prompting inquiries from U.S. and international lawmakers. As EPIC told Congress, "Facebook's admission that it

---

[10] Fed. Trade Comm'n., *In re Facebook*, Decision and Order, FTC File No. 092 3184 (Jul. 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.
[11] *Id.*
[12] Fed. Trade Comm'n, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, Press Release (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.
[13] *See, In the Matter of Facebook, Inc.* (EPIC, Complaint, Request for Investigation, Injunction, and Other Relief) before the Federal Trade Commission, Washington, D.C. (filed Dec. 17, 2009), http://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.
[14] *Id.*
[15] *Id.*

disclosed data to third parties without users' consent suggests a clear violation of the 2011 Facebook Order."[16] The U.K. Information Commissioner's Office recently fined Facebook the maximum allowable fine under U.K. law as the result of this data transfer, charging Facebook with "failing to safeguard people's information [and] failing to be transparent about how people's data was harvested by others and why they might be targeted by a political party or campaign."[17] The FTC has recently announced that it is investigating Facebook.[18] As the Acting Director of the Bureau of Consumer Protection stated:

> The FTC is firmly and fully committed to using all of its tools to protect the privacy of consumers. Foremost among these tools is enforcement action against companies that fail to honor their privacy promises, including to comply with Privacy Shield, or that engage in unfair acts that cause substantial injury to consumers in violation of the FTC Act. Companies who have settled previous FTC actions must also comply with FTC order provisions imposing privacy and data security requirements. Accordingly, the FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook. Today, the FTC is confirming that it has an open non-public investigation into these practices.[19]

Many State Attorneys General have also announced their investigations into the matter.[20]

Given Facebook's obligations under the FTC Consent Order and its continuing violations of user privacy, it is particularly troubling that you plan to move forward with plans to collect the data of 2.2 billion Facebook users without their consent. This proposal not only violates the FTC Consent Order, but the privacy rights of Facebook's 2.2 billion users.

The Social Science One study should be suspended pending a determination by the FTC regarding Facebook's compliance with the 2011 Consent Order.

III. Facebook's Prior Relations with Researchers Have Raised Significant Questions

Facebook has a sordid history of privacy violations when doing research, and Social Science One is inadequately prepared to protect the privacy of its research subjects. Social Science One represents that "All research projects must pass the standard peer-review protocols of academic social science, with the addition of a special ethical review designed for the unique challenges of

---

[16] Letter from EPIC to S. Comm on the Judiciary, (Apr. 9, 2018), https://epic.org/testimony/congress/EPIC-SJC-Facebook-Apr2018.pdf.

[17] Information Commissioner's Office, *Investigation Into the Use of Data Analytics In Political Campaigns*, (Jul. 10, 2018), https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf.

[18] Fed. Trade Comm'n., *Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices* (Mar. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer- protection.

[19] *Id.*

[20] *See*, EPIC, *State AGs Launch Facebook Investigation*, (Mar. 26, 2018), https://epic.org/2018/03/state-ags-launch-facebook-inve.html.

analyzing the types of questions and data."[21] As you are aware, Cambridge Analytica was able to exploit data because Facebook gave improper access to an academic researcher. Therefore, the fact that this research will be subject to standard peer-review protocols and Facebook's ethical review methods—as research using Facebook data has been subject to in the past—does not sufficiently address the privacy risks.

Facebook's record with researchers indicates a disregard for user privacy and consent. In 2012, Facebook conducted an experiment that secretly manipulated user emotions by seeing if exposing users to more positive or negative content in their News Feed would affect their posting behaviors.[22] This was done by running randomized A/B testing on Facebook's platform, and Social Science One has stated that it is considering using data from randomized A/B tests run on Facebook's platform in the future.[23] Social Science One has not adequately addressed the ethical mistakes Facebook has made in the past and indicated how it will conduct its research differently.

IV. Voting data are extremely sensitive

Data on an individual's political views and voting habits are among the most sensitive types of personal information. Social Science One plans to combine post-election surveys (from Mexico, Brazil, Sweden, United States, and India) with Facebook data to research the effect of social media on elections.[24] Anonymity is a fundamental aspect of voting rights in the U.S. and in many other countries. Matching data on how people voted with their detailed Facebook profiles threaten to undermine that fundamental right.

The public cares deeply about the confidentiality of their voting data. Last year the Presidential Election Commission sought to wrongfully obtain voter data from all 50 states for the alleged purpose of investigating voter fraud. There was a public outcry, and many states refused to turn over their voter rolls to the federal government. EPIC (and several other groups) sued the Commission because its collection of the personal data of millions of registered voters was an unconstitutional invasion of privacy and its failure to conduct a Privacy Impact Assessment violated the E-Government Act.[25] The Commission was disbanded following the public opposition and lawsuits.[26]

V. Violation of GDPR

The General Data Protection Regulation ("GDPR") applies to the processing of personal data that monitors the behavior of individuals within the European Union. The heightened requirements of the GDPR will apply to the research proposed by Social Science One, even if the processing occurs in the US.

---

[21] https://socialscience.one/overview
[22] EPIC, *In re Facebook (Psychological Study)*, https://www.epic.org/privacy/internet/ftc/facebook/psycho/.
[23] https://socialscience.one/future-datasets
[24] https://socialscience.one/future-datasets.
[25] *EPIC v. Commission*, https://epic.org/privacy/litigation/voter/epic-v-commission/.
[26] Executive Order 13820 (Jan. 3, 2018), https://epic.org/privacy/litigation/voter/epic-v-commission/EPIC-v-Commission-termination-exec-order-010318.pdf.

In particular, Article 9 of the GDPR stipulates that "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited." The profiles of 2.2 billion Facebook users encompass virtually all of these sensitive data categories, which require the strictest safeguards for processing under the GDPR, even for academic research purposes.

The scope and purposes of the research proposed by Social Science One fail to meet the exemption for the processing of special categories of personal data on academic research grounds.

Article 89(1) of the GDPR requires that "processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner..."

Article 9(2)(j) of the GDPR requires that the extent of processing sensitive data for the purposes of academic research shall only be allowed if adheres to Article 89(1) and is "proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

The emphasis lies on data minimization foremost, then strict pseudonymization. Social Science One's access to 2.2 billion Facebook users' data in no way demonstrates either safeguard to meet the requirements of the GDPR. Due to the immensity and granularity of data disclosed by Facebook, the purposes of safeguarding the fundamental rights and interests of the data subject can no longer be achieved by pseudonymization, or "de-identification."

First, the sheer extent of data available to Social Science One violates a fundamental tenet of the GDPR—data minimization (Article 5). The research groups have not taken any active steps to implement technical and organizational measures to limit the processing of sensitive data. By accepting access to this massive trove of sensitive personal information, the groups have also failed to adequately assess the risks to the rights and freedoms of individuals as per GDPR Recital 75, and violated the rights to information about processing and access to data for individuals (Articles 13 and 15). There remain significant risks for the unauthorized reversal of pseudonymization with catastrophic effects on the privacy of individuals. This already constitutes multiple violations of the GDPR.

Secondly, reports that the researchers will share access to Facebook's proprietary user data indicate that Social Science One has no technical or organizational measures in place to pseudonymize data to the standard required by the GDPR. Recital 29 requires "additional information for attributing the personal data to a specific data subject [to be] kept separately." The groups have not implemented this, as evidenced by today's Wall Street Journal report: "to determine which data sets to release, a half-dozen primary researchers will have broad access to Facebook's proprietary user data, said Gary King, a social science professor at Harvard University and one of the co-chairs of the research group."

Furthermore, Article 29 Working Party's Opinion 05/2014 on Anonymisation Techniques established that de-identification must be "irreversible." This is a higher bar than simply removing personally identifiable information such as names and birthdays from perhaps the most comprehensive dataset ever compiled. Therefore, this proposed study violates EU data protection laws and irresponsibly imperils the privacy rights of individuals.

Conclusion

This research initiative violates U.S. and European law. Social Science One should suspend its research until the FTC is able to complete a full investigation. You say that you intend to conduct this research "according to the highest standards of data privacy"[27] but there is not even a designated privacy official to help make this determination.

The concerns that EPIC has outlined in this letter are widely shared. We urge you to consider carefully the consequences of the misuse of personal data that may result from this undertaking.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Christine Bannan*
Christine Bannan
EPIC Administrative Law and Policy Fellow

/s/ *Sunny Kang*
Sunny Kang
EPIC International Consumer Counsel

/s/ *Sam Lester*
Sam Lester
EPIC Consumer Privacy Fellow

Cc: Commissioners of the US Federal Trade Commission
Chair of the European Union Data Protection Board

[27] https://socialscience.one/our-facebook-partnership

Before the
FEDERAL TRADE COMMISSION
Washington, DC

In the Matter of	)
	)
Facebook, Inc. and	)
Facial Recognition	)
	)

Complaint, Request for Investigation, Injunction, and Other Relief

Submitted by

The Electronic Privacy Information Center, The Campaign for a Commercial Free Childhood, The Center for Digital Democracy, The Constitutional Alliance, Consumer Action, The Consumer Federation of America, Consumer Watchdog, The Cyber Privacy Project, Defending Rights & Dissent, The Government Accountability Project, The Privacy Rights Clearinghouse, Patient Privacy Rights, The Southern Poverty Law Center, and The U.S. Public Interest Research Group

I. Introduction

1. This complaint concerns recent changes in Facebook's business practices that threaten user privacy and violate the 2011 Consent Order with the Federal Trade Commission. As set forth in detail below, Facebook now routinely scans photos for biometric facial matches without the consent of the image subject. Moreover, the company seeks to advance its facial recognition techniques by deceptively enlisting Facebook users in the process of assigning identity to photo images. This unwanted, unnecessary, and dangerous identification of individuals undermines user privacy, ignores the explicit preferences of Facebook users, and is contrary to law in several states and many parts of the world. The Commission must undertake an investigation, enjoin these unlawful practices, establish sanctions, and provide appropriate remedies.

2. The 2011 Consent Order is clear: Part I of the proposed order prohibited Facebook from misrepresenting the privacy or security of "covered information."[1] According to the proposed order, "'Covered information' is defined broadly as 'information from or about an individual consumer, including but not limited to: . . . (e) photos and videos. . .'"[2] Part II of the proposed order required Facebook to "give its users a clear and prominent notice and obtain their affirmative express consent before sharing their previously-collected information with third parties in any way that materially exceeds

[1] Federal Trade Commission, *Facebook, Inc.; Analysis of Proposed Consent Order To Aid Public Comment*, 76 Fed. Reg. 75883 (Dec. 5, 2011), https://www.ftc.gov/sites/default/files/documents/federal_register_notices/facebook-inc.analysis-proposed-consent-order-aid-public-comment-proposed-consent-agreement/111205facebookfrn.pdf.
[2] *Id.* (emphasis added).

the restrictions imposed by their privacy settings."[3] Part IV "requires Facebook to establish and maintain a comprehensive privacy program that is reasonably designed to: (1) Address privacy risks related to the development and management of new and existing products and services, and (2) protect the privacy and confidentiality of covered information. The privacy program must be documented in writing and must contain controls and procedures appropriate to Facebook's size and complexity, the nature and scope of its activities, and the sensitivity of covered information."[4]

3. Facebook violated the 2011 Consent Order in multiple ways. Facebook's changes to its facial recognition practices exposed users' covered information in a way that materially exceeded the restrictions imposed by their privacy settings. Moreover, Facebook did not provide users with clear and prominent notice nor obtain their affirmative express consent before enacting these changes. Facebook also misrepresented the privacy and security of covered information. Finally, Facebook failed to establish and maintain a comprehensive privacy program to address the privacy risks of new and existing products and to protect the privacy and confidentiality of covered information.

II. The Parties

4. The Electronic Privacy Information Center ("EPIC") is a not-for-profit research center based in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the Federal Trade Commission. The 2011 FTC Consent Order arises from a series of complaints filed by EPIC from 2009 to 2011 concerning material changes to privacy settings made by Facebook. EPIC has continued to advocate for the Commission's enforcement of consent decrees to ensure that companies adhere to their obligations to consumer privacy.

5. The Campaign for a Commercial Free Childhood ("CCFC") is a national advocacy organization dedicated to countering the harmful effects of commercialism on children. CCFC organizes campaigns against corporations that target children with harmful marketing, helps parents and professionals reduce the amount of time kids spend with ad-supported screens, and advocates for policies that limit marketers' access to children.

6. The Center for Digital Democracy ("CDD") is a not-for-profit D.C.-based organization focused on protecting consumers in the digital marketplace.[5] During the 1990's (and then operating as the Center for Media Education) its work to protect privacy on the Internet led to the passage of the Children's Online Protection Act (COPPA) by Congress in 1998.[6] CDD's advocacy on the Google-Doubleclick merger played a major role in the FTC's decision to address privacy concerns arising from

[3] *Id.* (emphasis added).
[4] *Id.* (emphasis added).
[5] Ctr. for Digital Democracy, *About CDD*, http://www.democraticmedia.org/about-cdd.
[6] Katherine C. Montgomery, *Generation Digital*, MIT Press, http://mitpress.mit.edu/books/generation-digital.

online behavioral advertising.[7] Through a series of complaints filed at the commission, CDD has brought attention to privacy concerns with mobile devices, real-time tracking and targeting platforms, social media, and from the databroker industry. CDD's four-year campaign to ensure that COPPA was effectively implemented across all major platforms and applications resulted in the FTC's December 2012 decision to strengthen its rules on children's privacy.

7. The Constitutional Alliance is the only national organization in the United States that specifically focuses on the issue of the use of biometrics, including but not limited to Facial Recognition Technology (FRT). We work with state lawmakers and Congress to educate our elected representatives on the risk to a free society, when FRT is used by government and corporations. The Constitutional Alliance opposes the use of biometrics by any company absent informed consent, which includes a customer/user must need to opt-in before their biometrics can be used. Further, the biometrics of an individual must not be able to be shared with other companies and/or entities without the knowledge and consent of the customer/user.

8. Consumer Action has been a champion of underrepresented consumers nationwide since 1971. A non-profit 501(c)(3) organization, Consumer Action focuses on consumer education that empowers low- and moderate-income and limited-English-speaking consumers to financially prosper. It also advocates for consumers in the media and before lawmakers to advance consumer rights and promote industry-wide change.

9. The Consumer Federation of America (CFA) is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.

10. Consumer Watchdog is a nonprofit, nonpartisan, public interest corporation organized to represent the interests of consumers and taxpayers. A core focus of Consumer Watchdog's Privacy and Technology Project is protecting people's online privacy and enabling them to have control over data about them.

11. The Cyber Privacy Project (CPP) addresses issues about privacy raised in a networked world. In upholding the belief that privacy is essential to democratic society, Cyber Privacy Project anchors its approach in realizing the beneficial potential of the Constitution, laws, and policies of the U.S. CPP calls for implementation of privacy protections based on First Amendment rights of privacy and anonymity, Fourth Amendment rights against unreasonable searches and seizures, the Fifth and Fourteenth Amendment rights to due process and protection of liberty, and Article IV Privileges and Immunities to Travel and Work. It also calls upon similar principles in international human rights documents, state constitutions, and codes of ethics. CPP particularly questions the proliferation of digital

[7] Louise Story, *F.T.C. Approves Doubleclick Deal*, N.Y. Times, Dec. 21, 2007, at C3, http://www.nytimes.com/2007/12/21/business/21adco.html.

photography requirements, interoperability and recognition as magnifying privacy violations.

12. Defending Rights & Dissent ("DRAD") is a not-for-profit public education and advocacy organization based in Washington, DC. The mission of the organization is to strengthen participatory democracy by protecting the right to political expression. The ability to safeguard one's privacy is recognized as an important factor in protecting free speech and expression. Given the role of Facebook as a modern-day town square where matters of public concern are debated, DRAD is concerned that continued violations of user's privacy by Facebook adversely impact the rights of Facebook users to freely engage in political expression.

13. The Government Accountability Project ("GAP") is a non-profit, non-partisan public interest organization that promotes government and corporate accountability by litigating whistleblower cases, publicizing whistleblowers' concerns, and developing legal reforms to support the rights of employees to use speech rights to challenge abuses of power that betray the public trust. GAP, as an organization committed to protecting the public from the effects of an unaccountable institutions—illegality, corruption, abuses of authority, and dangers to fundamental public interests—joins this Complaint.

14. Patient Privacy Rights (PPR) was founded in 2004 by Deborah C. Peel, MD. Our mission is to honor and empower the individual's right to privacy through personal control of health information wherever such information is collected and used. Patient Privacy Rights educates, collaborates and partners with people to ensure privacy in law, policy, technology, and maximize the benefits from the use of personal health information with consent. PPR is recognized as the world's most prominent human and civil rights organization dedicated to restoring health privacy. PPR projects include leading a bipartisan coalition of 50+ organizations representing 10.3M people who want to control personal health data. The coalition successfully pressed for tough new penalties for data breaches and new privacy protections in HITECH and other federal regulations.

15. The Privacy Rights Clearinghouse (PRC) is a 501(c)(3) nonprofit consumer education and advocacy organization, located in San Diego, California. Established in 1992, PRC's mission is to engage, educate, and empower consumers to protect their privacy. PRC publishes extensive consumer education resources, provides one-to-one assistance, and advocates for strong privacy protections.

16. The Southern Poverty Law Center (SPLC) is a not-for-profit organization that uses litigation, education, and other forms of advocacy to fight hate, discrimination, and other forms of unfairness. In 2017, it launched a digital literacy campaign to provide tools and lesson plans to help educators teach their students about, among other things, the impact of online activity on their personal privacy and about how companies mine social media data. The SPLC is also concerned about the possible misuse of social media data for law enforcement purposes.

17. U.S. Public Interest Research Group serves as the national federation of state PIRGs, which are non-profit, non-partisan public interest advocacy organizations that take on powerful interests on behalf of their members. U.S. PIRG has long advocated at the state and national level for greater consumer control of their information, greater data security and greater accountability for data collectors. U.S. PIRG has filed, or co-filed, numerous petitions and complaints to the FTC on issues including data brokers, the Internet ecosystem and the general sharing, selling and scoring of personal information.

III. The Privacy Risks of Facial Recognition

18. Facial recognition systems include computer-based biometric techniques that detect and identify human faces.[8]

19. The National Academy of Sciences has stated:

> The success of large-scale or public biometric systems is dependent on gaining broad public acceptance of their validity. To achieve this goal, the risks and benefits of using such a system must be clearly presented. Public fears about using the system, including . . . concerns about theft or misuse of information, should be addressed.[9]

20. There is significant controversy surrounding the use of facial recognition technology. Private companies covertly deploy facial recognition techniques to obtain the identity of unsuspecting individuals. For example, Madison Square Garden deploys facial recognition on attendees at public sporting events:[10]

> The technology uses cameras to capture images of people, and then an algorithm compares the images to a database of photographs to help identify the person and, when used for security purposes, to determine if the person is considered a problem. The technology, which is sometimes used for marketing and promotions, has raised concerns over personal privacy and the security of any data that is stored by the system.

21. Commercial deployment of facial recognition is also pervasive in the advertising industry. For example, Unilever has utilized facial scanning to measure shoppers' emotional engagement with on-shelf displays.[11]

---

[8] EPIC, *Facial Recognition*, http://epic.org/privacy/facerecognition/; *see also* John D. Woodward, et al, Rand, *Biometrics: A Look at Facial Recognition* 8-9 (2003), *available at* http://www.rand.org/content/dam/rand/pubs/documented_briefings/2005/DB396.pdf.

[9] National Academy of Sciences, *Biometric Recognition: Challenges and Opportunities (Report in Brief)* 7 (2010), *available at* http://sites.nationalacademies.org/cstb/CurrentProjects/CSTB_059722.

[10] Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y. Times, Mar. 13, 2018, at B8, https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html.

[11] Michael Barnett, *Unilever trials in-store facial recognition technology*, Marketing Week, (Mar. 7, 2018), https://www.marketingweek.com/2018/03/07/unilever-in-store-facial-recognition/.

22. EPIC's Jeramie Scott has explained the privacy and surveillance issues of commercial deployment of facial recognition:[12]

> As large institutions begin using facial recognition on the public, it normalizes a privacy-invasive technology that lacks meaningful safeguards. The lack of regulation of facial recognition and other biometric surveillance methods means the data collected and used now for one purpose can easily be utilized for purposes not even imagined yet and without the consent from the targets of the technology. Each instant where mass surveillance is implemented, especially where little to no regulation exists like it does with facial recognition, takes us one step closer to ubiquitous surveillance and one step farther from the liberties we are supposed to hold dear.

23. The use of facial recognition technology by governments also raise significant privacy concerns.

24. The United States Custom and Border Protection ("CBP"), Department of Homeland Security ("DHS"), and the Federal Bureau of Investigation ("FBI") coordinate various programs on facial recognition technology that raise substantial privacy and civil liberties concerns.

25. Facial recognition technology can be done covertly, even remotely, and on a mass scale. There is little that individuals can do to prevent collection of one's image. Participation in society involves exposing one's face. Ubiquitous and near effortless identification eliminates individuals' ability to control their identities and poses a special risk to the First Amendment rights of free association and free expression, particularly to those who engage in lawful protests.

26. Governments around the world seek access to images of political organizers to obtain actual identities and to enable investigation and prosecution.

27. In Canada, police coordinated with the Canadian Bankers Association to deploy facial recognition software to identify protestors at the 2010 G20 summit in Toronto.[13]

28. In Iran, government agents have posted pictures of political activists online and used "crowd-sourcing" to identify individuals.[14] There is also evidence that Iranian

---

[12] Dave Zirin and Andrew Tan-Delli Cicchi, *Fans Are the Target of Madison Square Garden's New Facial-Recognition Technology: Facial recognition is a threat to privacy and the latest frontier in surveillance, The Nation* (Mar. 23, 2018),, https://www.thenation.com/article/fans-are-the-target-of-madison-square-gardens-new-facial-recognition-technology/.

[13] Ashley Csanady, *Police using facial recognition software to help ID G20 suspects*, National Post, (Jul. 15, 2010), http://nationalpost.com/posted-toronto/police-using-facial-recognition-software-to-help-id-g20-suspects.

[14] Robert Mackey, *The Lede: Updates on Iran's Disputed Election*, N.Y. Times, Jun. 24, 2009, , http://thelede.blogs.nytimes.com/2009/06/24/latest-updates-on-irans-disputed-election-5/.

researchers are working on developing and improving facial recognition technology to identify political dissidents.[15]

29. Facebook currently grants government access to user information on merely a "good faith belief" that the disclosure is required by law or when it is necessary to protect Facebook from people it believes are violating its "Statement of Rights of Responsibilities."[16]

30. Following earlier efforts by consumer privacy organizations, the FTC acknowledged the privacy concerns raised by the commercial use of facial recognition:

> [T]he use of facial recognition technologies can raise privacy concerns. For example, panelists voiced concerns that databases of photos or biometric data may be susceptible to breaches and hacking. Further, panelists discussed how some consumers may perceive digital signs equipped with cameras using facial recognition technologies as invading their privacy because they can detect consumers from a distance and process their images without their knowledge or consent."
>
> Perhaps of most concern, panelists surmised that advances in facial recognition technologies may end the ability of individuals to remain anonymous in public places. For example, a mobile app that could, in real-time, identify anonymous individuals on the street or in a bar could cause serious privacy and physical safety concerns, although such an app might have benefits for some consumers. Further, companies could match images collected by digital signs with other information to identify customers by name and target highly-personalized ads to them based on past purchases, or other personal information available about them online. Social networks could identify non-users of the site – including children – to existing users, by comparing uploaded images against a database of identified photos.[17]

31. EPIC has previously advised the Commission that, "[c]entral to the meaningful safeguards to face recognition technology are (1) subject control over image enrollment, (2) subject control over the processing and identification of images, (3)

---

[15] Melika Abbasian Nik, Mohammad Mahdi Dehshibi, and Azam Bastanfard, *Iranian Face Database and Evaluation with a New Detection Algorithm*, In Proc. of 2nd BEC (2007) http://dehshibi.com/files/papers/Iranian%20Face%20Database%20and%20Evaluation%20with%20a%20new%20detection.pdf.

[16] Facebook, Privacy Policy, http://www.facebook.com/policy.php.

[17] Fed. Trade Comm'n, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, (Oct. 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

transparency in the functioning, use, and purpose of the facial recognition system, and (4) independent accountability of the image processing entity.[18]

32. Facebook has failed to adopt one or more of these safeguards in violation of the 2011 FTC Consent Order.

IV. Facebook's Deployment of Facial Recognition Techniques

A. Facebook's Size and Reach Are Unparalleled Among Social Networking Sites

33. Facebook is the largest social network service provider in the United States. There are over 2.13 billion monthly active Facebook users worldwide, of whom 214 million are American.[19]

34. Approximately 350 million photos are uploaded every day, with 14.58 million photo uploads per hour.[20]

B. Facebook's Early Development of Facial Recognition Technology Was Dependent on Collecting Biometric Data on Users Without Knowledge or Consent

35. Facebook's facial recognition technology works by generating a biometric signature for users who are tagged in photos on Facebook, i.e. using "summary data" from "photo comparisons." This representation of biometric information, based on the user's facial image is available to Facebook but not to the user.

36. Facebook collects facial recognition data through a deceptive practice: it suggests a tag identifying a user, for the user to confirm by approving the suggestion. Facebook routinely encourages users to "tag," others, i.e. provide actual identifying information about themselves, their friends, and other people they may recognize. Facebook does not explain that this practice enables the company to identify images in other contexts.

37. Facebook associates the tags with a user's account, compares what these tagged photos have in common and stores a summary of this comparison.

38. Facebook compares uploaded photos "to the summary information we've stored about what your tagged photos have in common."

39. Facebook's Help Center describes this technology as "[analyzing] the pixels in photos and videos, such as your profile picture and photos and videos that you've been tagged in, to calculate a unique number, which we call a template. We compare other

---

[18] EPIC, *In the Matter of Facebook, Inc. and the Facial Identification of Users (EPIC Complaint, Request for Investigation, Injunction, and Other Relief*) (Jun. 10, 2011), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf.

[19] *See,* Zephoria Digital Marketing, *The Top 20 Valuable Facebook Statistics – Updated March 2018,* https://zephoria.com/top-15-valuable-facebook-statistics/.

[20] *Id.*

photos and videos on Facebook to this template and if we find a match we'll recognize you."[21]

40. The Tag Suggestions technology identifies users in photos without their consent. However, Facebook gave no clear and conspicuous notice to users and failed to obtain meaningful express consent prior to collecting "Photo Comparison Data," generating unique biometric identifiers, and linking biometric identifiers with individual users.

41. Facebook's subsequent facial recognition technique ("2018 Facial Recognition Practice") notifies users when their biometric face print is detected on an image, even if it has not been tagged by another user.

42. The 2018 Facial Recognition Practice derives biometric data from Facebook users in a materially different manner than Facebook represented when they first collected the data using Tag Suggestions.

C. Facebook Never Obtained Affirmative Express Consent for Any Use of Facial Recognition Technology and Continues to Benefit from its Privacy Misrepresentations

43. Facebook never obtained "affirmative express consent" for its deployment of facial recognition, as required by Part II of the 2011 Consent Order. The Commission's analysis of the Order makes clear that Facebook must "give its users a clear and prominent notice and obtain their affirmative express consent before sharing their previously-collected information with third parties in any way that materially exceeds the restrictions imposed by their privacy settings."[22]

44. Since 2010, Facebook deployed extensive facial recognition practices on an opt-out basis without providing clear and conspicuous notice, without obtaining users' affirmative express consent, and without effectively guiding users on how to opt-out of the default Tag Suggestions setting.

45. In 2013, Facebook abruptly lifted its brief suspension of the Tag Suggestions program despite significant backlash, and automatically reinstated it for every user in the United States.

46. A review of the company's approach to facial recognition from 2010 to 2018 clearly invalidates any claim of implied or continuing consent that could justify the implementation of the 2018 Practice without renewed and affirmative consent.

i. No User Consent Obtained for Tag Suggestions in 2010-2011

47. In 2010, Facebook announced face detection technology for photos:

---

[21] Facebook, Help Center, *How does Facebook's face recognition work?*, https://www.facebook.com/help/218540514842030.

[22] Facebook, Inc., Proposed Consent Order (emphasis added).

> You now can add tags with just a couple of clicks directly from your home page and other sections of the site, using the same face detection technology that cameras have used for years… With this new feature, tagging is faster since you don't need to select a face. It's already selected for you, just like those rectangles you see around your friends' faces when you take a photo with a modern digital camera. All that's left for you to do is type a name and hit enter.[23]

48. Facebook subsequently announced in 2010 a bulk tagging technology for photos:

> When people upload a set of photos, they are often of events like weddings and birthday parties where people are with the same group of friends and family. With our new uploader, you will be able to tag multiple photos in the same album all at once, as well as tag photos of the same person with a lot less effort.[24]

49. At the outset, Sam Odio, Facebook Photo Products Manager, attempted to distinguish Facebook's "face detection" and "bulk tagging" techniques from facial recognition technology:

> This isn't face recognition… Picasa and iPhoto--they'll detect a face and say, "This is Sam," and they'll suggest that it's Sam. We're not doing that. We're not linking any faces to profiles automatically. Right now, we want to stay away from that because it's a very touchy subject.[25]

50. In 2011, Facebook's Justin Mitchell revised the characterization of photo tagging Facebook Photos, acknowledging that Facebook was now deploying "face recognition" techniques.

> When you or a friend upload new photos, we use face recognition software—similar to that found in many photo editing tools—to match your new photos to other photos you're tagged in. We group similar photos together and, whenever possible, suggest the name of the friend in the photos. If for any reason you don't want your name to be suggested, you will be able to disable suggested tags in your Privacy Settings. Just click 'Customize Settings' and 'Suggest photos of me to friends.' Your name will no longer be suggested in photo tags, though friends can still tag you

[23] Sam Odio, *Making Photos Better*, Facebook Blog (Jul. 1, 2010), http://blog.facebook.com/blog.php?post=403838582130.
[24] Sam Odio, *More Beautiful Photos*, Facebook Blog (Sept. 30, 2010), http://blog.facebook.com/blog.php?post=432670242130.
[25] Caroline McCarthy, *Facebook Photos Get High Resolution, Bulk Tagging*, CNET (Sept.30, 2010), https://www.cnet.com/news/facebook-photos-get-high-resolution-bulk-tagging/.

> manually. We notify you when you're tagged, and you can untag yourself at any time. As always, only friends can tag each other in photos.[26]

51. Facebook later announced that it had deployed "Tag Suggestions" technology over the last several months, and that the technology had been available internationally. Facebook did not provide users with any other notice about this facial recognition technology.[27]

52. Facebook admitted in a later statement, that "we should have been more clear during the roll-out process when this became available to them."[28] (At the date of this complaint, the blog post apologizing for user confusion in the roll-out process of Tag Suggestions has been removed from Facebook Newsroom.)

53. However, in each subsequent deployment of facial recognition techniques for the ensuing eight years, Facebook has made no effort to rectify that matter or to allow users to opt-in if they so choose.

54. Facebook's automated identification of facial images continues to occur in the absence of any user intervention.

55. Facebook enables Tag Suggestions by default; users may opt-out if they are aware of the default setting, but do not affirmatively opt-in to Tag Suggestions or subsequent facial recognition techniques.

ii. Post-FTC Consent Decree, 2013: Facebook Automatically Reinstated Tag Suggestions without User Consent

56. In 2012, Facebook was questioned by the Senate Judiciary Subcommittee on facial recognition technology.[29] In response to a question on why the platform does not implement an opt-in choice for users rather than turning on Tag Suggestions by default, Facebook Privacy and Policy manager Rob Sherman answered:[30]

> Facebook itself is an opt-in experience. People choose to be on Facebook because they want to share with each other. We think that it's the right choice to let people who are uncomfortable with it to decide to opt out.

---

[26] Justin Mitchell, *Making Photo Tagging Easier*, Facebook Blog, (June 7, 2011), http://blog.facebook.com/blog.php?post=467145887130.

[27] Tiffany Kaiser, *Facebook Prompts More Privacy Anxieties with Facial Recognition Feature,* DailyTech, June 8, 2011, http://www.dailytech.com/Facebook+Prompts+More+Privacy+Anxieties+with+Facial+Recognition+Feature/article21848.htm?.

[28] Alexei Oroskovic, *Facebook Facial Recognition Technology Sparks Renewed Concerns,* Reuters, June 8, 2011, http://www.reuters.com/article/2011/06/08/us-facebook-idUSTRE7570C220110608.

[29] Ricardo Bilton, *Facebook hit with tough questions on facial recognition in Senate hearing* (July 18, 2012), Venture Beat, https://venturebeat.com/2012/07/18/facebook-hit-with-tough-questions-on-facial-recognition-in-senate-hearing/.

[30] *Id.*

57. This response was heavily scrutinized by Senator Blumenthal and Senator Franken for deflecting the question on Facebook's lack of informed choice mechanisms that enable users to fully understand their enrollment in facial recognition, the privacy implications of the technology, and to easily withdraw from tag suggestions.[31]

58. The Office of the Data Protection Commissioner, Ireland published a comprehensive assessment of Facebook's data practices as part of an audit to investigate Facebook's compliance with European privacy laws.[32] As a result of scrutiny from European data protection regulators, Facebook discontinued facial recognition by automatic photo tagging in Europe.[33]

59. In late 2012, Facebook temporarily suspended Tag Suggestions in the United States after significant public backlash by consumer privacy groups. In a press release, Facebook claimed that it will "make improvements to the tool's efficiency" without specifying when or how Tag Suggestions will be re-engineered to address salient user privacy concerns.

60. In 2013, Facebook automatically reinstated Tag Suggestions for users in the United States without any additional safeguards to address consumer privacy concerns. Tag Suggestions were enabled by default for every user in America.[34]

---

[31] T.C. Sottek, *Senator Al Franken grills FBI, Facebook, and others on facial recognition technology*, The Verge, July 18, 2012, https://www.theverge.com/2012/7/18/3167864/senator-al-franken-fbi-facebook-facial-recognition-hearing.

[32] Data Protection Commissioner, *Report of Review of Facebook Ireland's Implementation of Audit Recommendations Published – Facebook turns off Tag Suggest in the EU*, https://www.dataprotection.ie/docs/21-09-12-Press-Release--Facebook-Ireland-Audit-Review-Report/1233.htm; *see also,* EPIC, *EPIC Recommends Safeguards For Facial Recognition Technology,* https://epic.org/2014/02/epic-recommends-safeguards-for.html.

[33] Somini Sengupta and Kevin O'Brien, *Facebook Can ID Faces, but Using Them Grows Tricky* N.Y. Times, Sept. 21, 2012, at A1, https://www.nytimes.com/2012/09/22/technology/facebook-backs-down-on-face-recognition-in-europe.html.

[34] Emil Protalinski, *Facebook re-enables Tag Suggestions facial-recognition feature in the US, on by default for all* The Next Web, Feb. 1, 2013, https://thenextweb.com/facebook/2013/02/01/facebook-re-enables-tag-suggestions-facial-recognition-feature-in-the-us-on-by-default-for-all/; Paul Ducklin, *Facebook is turning facial recognition back on – so here's how to check your "photo tagging" settings* Naked Security, Feb. 2, 2013, https://nakedsecurity.sophos.com/2013/02/02/facebook-turns-facial-recognition-back-on/.

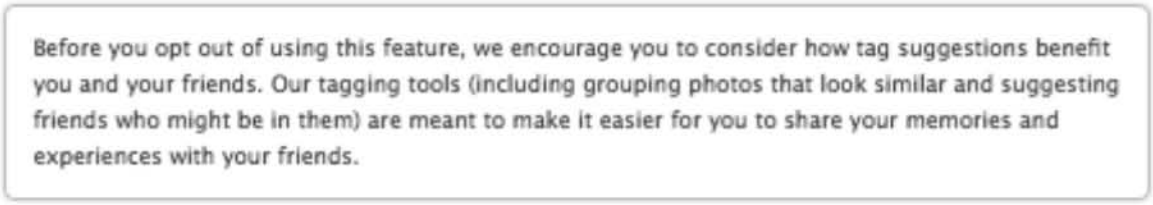
61. On the "Facebook and Privacy" page, Facebook admitted that the reinstated Tag Suggestions was the "same feature that millions of people previously used to help them quickly share billions of photos with friends and family." Facebook did not explicitly clarify that Tag Suggestions remained opt-out for users or explain the privacy implications of the default setting.

62. The hyperlink to "learn more about tag suggestions and how to control them" did not direct the user to a clear and conspicuous opt-out setting. An archive of the page on February 1, 2013 shows that the hyperlink led to Facebook's Help Center with a list of FAQs on "Tagging Photos." The term "facial recognition" was not used at all.

63. Users had to scroll down to the end of the page to locate "How can I turn off tag suggestions for photos of me?" Clicking on this link still did not direct the user to a clear and conspicuous opt-out setting. Instead, the page set out a 4-step instruction on how to navigate the user's privacy settings to exercise opt-out.

64. Facebook actively discouraged users from opting out with a disclaimer that read:

> Before you opt out of using this feature, we encourage you to consider how tag suggestions benefit you and your friends. Our tagging tools (including grouping photos that look similar and suggesting friends who might be in them) are meant to make it easier for you to share your memories and experiences with your friends.



65. Facebook never obtained affirmative express consent to reinstate Tag Suggestions in 2013, and it actively convoluted the process of opting-out to discourage users from disabling facial recognition settings.

66. Facebook's claim to "respect users' existing privacy settings" in rolling out the 2018 Facial Recognition Practice is misleading and deceptive, and also constitutes a violation of the FTC Consent Decree.

iii. Post-FTC Consent Decree, 2014: Facebook Developed DeepFace Facial Recognition Technology from Analyzing User Photos

67. In 2014, Facebook and its subsidiary Face.com published a research paper on DeepFace.[35] Facebook presented DeepFace at the IEEE Conference on Computer Vision and Pattern Recognition in June 2014.

68. At present, the post on https://research.fb.com/, entitled "Closing the Gap to Human Level Performance in Face Verification" has been deleted from Facebook.[36]

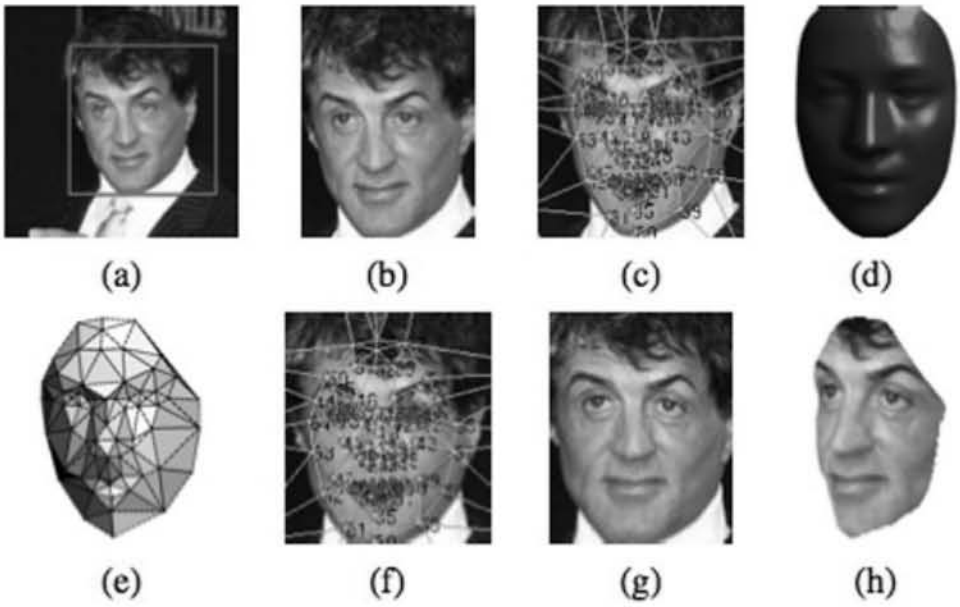
69. DeepFace is an artificial intelligence system that trained on 4 million photos "from a popular social network" to match different images of the same person using their biometric face print. The research claimed an accuracy rate of 97.25 percent, even when the images presented contextual differences in angle, lighting, and facial expressions.[37]

---

[35] Tom Simonite, *Facebook Creates Software That Matches Faces Almost as Well as You Do* MIT Tech. Rev., (Mar. 17, 2014), https://www.technologyreview.com/s/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/.

[36] "404 Page Not Found. It looks like nothing was found at this location,", https://research.fb.com/search?q=%22DeepFace%3A+Closing+the+Gap+to+Human-Level+Performance+in+Face+Verification%22.

[37] Will Oremus, *Facebook's New Face-Recognition Software Is Scary Good*, Slate, Mar. 18, 2014, http://www.slate.com/blogs/future_tense/2014/03/18/deepface_facebook_face_recognition_software_is_97_percent_accurate.html.



70. Facebook's unprecedented access to extensive biometric data on users enabled its facial recognition capacity to surpass the accuracy of systems deployed by law enforcement and the FBI in 2014.[38]

71. Facebook spokeswoman Lydia Chan claimed in 2014 that, "this is theoretical research, and we don't currently use the techniques discussed in the paper on Facebook."[39]

72. However, the research relied on Facebook's user data to expand the neural network of the machine learning system to increase DeepFace's facial recognition capabilities.

73. The 2018 Facial Recognition Practice, which scans for a user's biometric face print on any photo uploaded to Facebook—viewable by that user with or without tags—demonstrates that Facebook is indeed commercially deploying its facial recognition technology beyond research purposes and outside the scope of what is permitted under the 2011 Consent Decree.

[38] Russell Brandom, *Why Facebook is beating the FBI at facial recognition*, The Verge, July 7, 2014, https://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition.
[39] Will Oremus, *supra*; *see also,* James O'Toole, *Facebook's new face recognition knows you from the side*, CNN Tech, Apr. 4, 2014, http://money.cnn.com/2014/04/04/technology/innovation/facebook-facial-recognition/index.html.

iv. Post-FTC Consent Decree, 2017-2018: Facebook Has Deployed Additional Facial Recognition Technology In Violation of State Biometric Information Privacy Laws

74. Facebook currently faces a class action lawsuit alleging that it violated the Illinois Biometric Information Privacy Act (BIPA) when it implemented the Tag Suggestions technology to extract biometric data without obtaining affirmative consent. [40]

75. The United States District Court for the Northern District of California denied Facebook's motion to dismiss for lack of standing, explaining, "Facebook insists that the collection of biometric information without notice or consent can never support Article III standing without 'real-world harms' such as adverse employment impacts or even just 'anxiety.' That contention exceeds the law." [41]

76. Despite the court's ruling, Facebook continues to disregard not only its obligation under the FTC Consent Order but the laws of several states, including Illinois, Texas and Washington.[42]

77. Facebook has continued to misrepresent its collection, use and disclosure of biometric data knowing that state laws prohibit the use of facial recognition without affirmative, express opt-in consent.

D. No Affirmative Consent Sought in 2017-2018 to Materially Change the Use of Facial Templates and to Gain More Rights to Collect Biometric Data

i. Discloses Non-Public Information in a Matter That Materially Exceeds Current Privacy Settings

78. The 2011 FTC Consent Order defines nonpublic user information as "covered information that is restricted by one or more privacy settings."

79. Facebook's updated setting notifies users to "find" photos that they are in but have not been tagged, as long as the photo's privacy settings allow the user to view it as a Friend, Public, or Custom Audience.

80. For example: User A posts a picture and applies the privacy setting of "Friends Only" and does not tag anyone; although this is non-public information under the 2012 Consent Order, User B, who is a friend of User A but has not been invited to share the content via a tag, will be notified of a facial recognition match.

81. Facebook has implemented changes to the facial recognition technology that materially exceeds users' current privacy settings. As detailed below, this constitutes several violations of the 2011 FTC Consent Order due to Facebook's insufficient

---

[40] *In re Facebook Biometric Information Privacy Litig.*, No 3:15-CV-03747-JD, *Order Re Renewed Mot. to Dismiss*, Dkt. No. 227 at 1, 5-7 (N.D. Cal Feb. 26, 2018).
[41] *Id.*
[42] *See,* Tex Bus & Com § 503.001; Wash. Rev. Code Ann. § 40.26.020 (2017).

notice to users on the privacy implications of additional facial recognition and its failure to obtain affirmative express consent.

ii. Consent Decree Violations by Misrepresentation and Failure to Obtain Affirmative Express Consent

82. Part II(B) of the 2011 FTC Consent Order requires Facebook to "obtain the user's affirmative express consent" prior to disclosing a user's nonpublic user information by [Facebook] with any third party, which materially exceeds the restrictions imposed by a user's privacy settings.[43]

83. Part I(A)-(B) of the 2011 FTC Consent Order prohibits Facebook from misrepresenting "in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to:[44]

> A. its collection or disclosure of any covered information;
>
> B. the extent to which a consumer can control the privacy of any covered information maintained by Respondent and the steps a consumer must take to implement such controls.

84. According to a report by WIRED, Facebook spokesperson Rochelle Nadhiri stated that "the new setting is not on by default." Nadhiri said, "[t]he new setting respects people's existing choices, so if you've already turned off tag suggestions then your new face recognition setting will be off by default. If your tag suggestions setting was set to 'friends' then your face recognition setting will be set to on."[45]

85. This representation is misleading to consumers. Functionally, Facebook's 2018 changes to facial recognition automatically applied to a majority of users who were enrolled into Tag Suggestions by default in 2013.

86. Tag Suggestions dates back five years. Many users remain unaware that Tag Suggestions applied to them by default in 2013, and that there is a choice to opt-out. Therefore, Facebook's reliance on this prior setting to infer consent for invasive changes to biometric data practices gives Facebook unprecedented control over facial templates without affirmative express consent.

87. Facebook's recent notice to users on the changes to the extent of facial recognition does not "conspicuously" present an opt-out button, but merely links a "Go to Settings" button.

---

[43] Fed Trade Comm'n, *In re Facebook*, Decision and Order, FTC File No. 092-3184 (Jul. 27, 2012) (Hereinafter "Facebook Consent Order").
[44] *Id.*
[45] Lily Hay Newman, *How to Turn Off Facebook's Face Recognition Features*, Wired, Feb. 28, 2018, https://www.wired.com/story/how-to-turn-off-facebook-face-recognition-features/.

88. This lack of clear and conspicuous notice violates Part I(A)-(B) of the Consent Order by misrepresenting "the extent to which a consumer can control the privacy of any covered information maintained by Respondent and the steps a consumer must take to implement such controls." Specifically, Facebook misrepresents the extent to which users can control the privacy of biometric information, and the extent of Facebook's collection and disclosure of the facial templates and photo comparison data to third parties.

89. Facebook violated Part II(B) of the Consent Order by failing to obtain affirmative express consent before implementing business changes to facial recognition techniques. Any claims of inferred or continuing consent from the user's prior setting on Tag Suggestions is invalid, as Facebook has never given users a choice to opt-in to facial recognition.

E. Users Were Not Clearly and Prominently Notified of Facebook's Changes to Facial Recognition Practices

90. Part II(A) of the 2012 FTC Consent Order requires Facebook to:

> Clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user…prior to any sharing of a user's nonpublic user information by [Facebook] with any third party, which materially exceeds the restrictions imposed by a user's privacy settings.

91. The Consent Order defines "clear and prominent" to mean:

> A. In textual communications (e.g., words displayed on the screen of a computer or mobile device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;
>
> C. In communications disseminated through video means… the required disclosures shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them
>
> D. In all instances, the required disclosures: (1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any statement contained within the disclosure or within any document linked to or referenced therein.

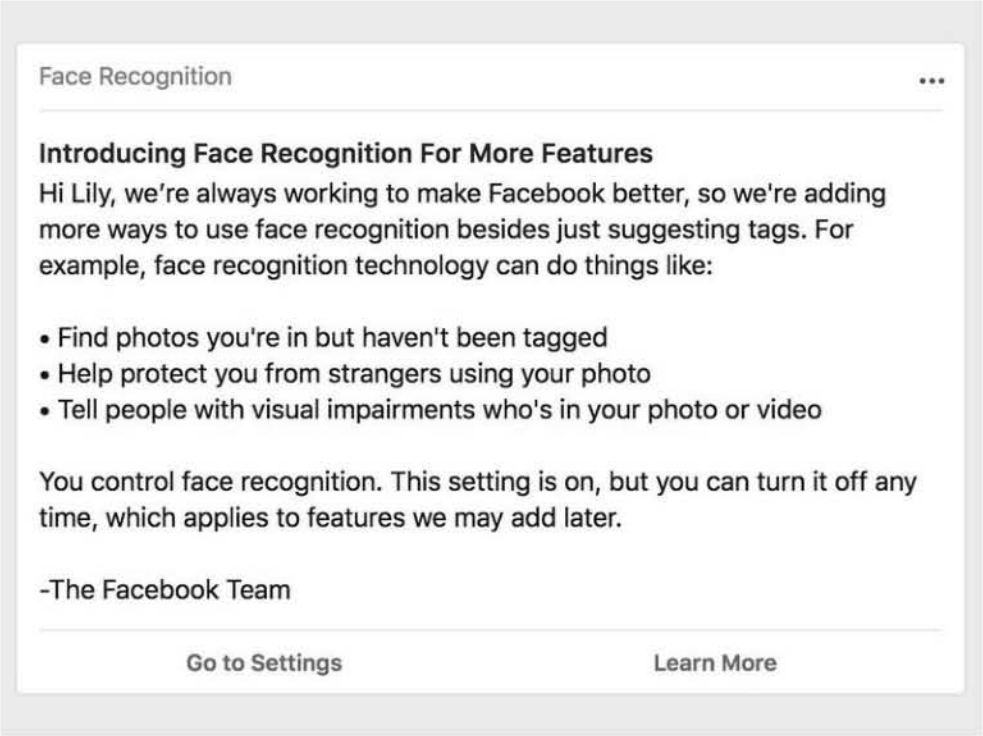
92. Facebook violated this provision and failed to meet the standards of a "clear and prominent" notice for the reasons detailed below.

i. Facebook's Announcement was Difficult to Locate and Notice

93. From December 2017 to early 2018, Facebook posted a short notice regarding its revised facial recognition practice through a disclaimer that appeared on users' news feeds.

94. The FTC requires truthful disclaimers to be displayed clearly and conspicuously, but Facebook's notice was buried in the densely packed text of users' news feeds.[46]

95. The brief post appeared at the top of users' news feeds, but did not make clear that Facebook had in fact changed users' privacy settings.



96. Facebook did not ensure that the notice appeared on screen for a duration sufficient for an ordinary consumer to notice, read, and comprehend. Users could easily scroll down on their mobile or computer device and miss out on the notice.

97. If the user continued to scroll down without having read the announcement, it was difficult to re-locate the disclaimer and the "Learn More" hyperlink to Facebook's press release on the implications of facial recognition technology.

98. Moreover, the buried notice on the news feed actually disappeared if a user refreshed the page.

[46] Fed. Trade Comm'n, *.com Disclosures*, (Mar. 2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.

99. As the change "rolled-out" to Facebook users gradually, users received notice at different times. The impact of Facebook's announcement on December 19, 2017 dissipated when some users were being notified in early January 2018, while others were not aware until mid-March 2018.

ii. Privacy Misrepresentations and Vagueness in the Announcements

100. Facebook's announcements of the change in facial recognition practice include significant misrepresentations and omissions, contrary to the requirements of the Consent Order.

101. On December 19, 2017, Facebook's Deputy Chief Privacy Officer Rob Sherman posted a blog post, entitled "Hard Questions: Should I Be Afraid of Face Recognition Technology?"[47]

102. On the potential risks of facial recognition technology, Sherman wrote:

> This tension isn't new. Society often welcomes the benefit of a new innovation while struggling to harness its potential. "Beware the Kodak," one newspaper intoned in 1888 as inexpensive equipment came onto the market making photography available to the masses. They called it a "new terror for the picnic." Confronting amateur photography for the first time, society could have restricted this technology – and fundamentally changed the way history was documented for more than a century.

103. The statement misleadingly equates highly sophisticated AI techniques, which can extract the exact biometric dimensions of a face, with the early development of film photography.

104. Facebook's announcement does not acknowledge the serious privacy implications of a large-scale, social media deployment of instantaneous facial recognition on the personal data of billions.

105. On Facebook's decision to adopt the business change on an opt-out basis, Sherman wrote:

> When we first introduced this feature in 2010, there was no industry standard for how people should be able to control face recognition. We decided to notify people on Facebook and provide a way to disable it in their account settings at any time … Just as in 2010, we had to evaluate how we'd inform people and give them choice over these new uses of the technology.

---

[47] Rob Sherman, *Hard Questions: Should I Be Afraid of Face Recognition Technology?* Facebook Newsroom, (Dec. 19, 2017), , https://newsroom.fb.com/news/2017/12/hard-questions-should-i-be-afraid-of-face-recognition-technology/.

106. This is a significant misrepresentation and an omission of Facebook's regulatory obligations to the FTC under the Consent Order.

107. After the FTC settlement in 2011, Facebook was not at liberty to self-evaluate and unilaterally enact significant changes in privacy practices. The Consent Order requires Facebook to adhere to specific regulatory guidelines on obtaining affirmative consent to change privacy settings.

108. The announcement also failed to mention that in 2013, Facebook automatically applied "Tag Suggestions" to all users by default—and that if users did not opt-out of Tag Suggestions in their privacy settings, the extended facial recognition practice would automatically apply to them without consent.

109. WIRED Security Reporter Lily Hay Newman criticized this setting:

> But the "tag suggestions" preference dates back more than four years. Even if you fully understood enough about face-recognition technology at the time to make a carefully considered choice in 2013, that doesn't necessarily mean you'll be fine letting even more of it into your life now.[48]

110. Contrary to Part I(B) of the 2011 FTC Consent Order, Facebook has consistently misrepresented "the extent to which a consumer can control the privacy of any covered information maintained by [Facebook] and the steps a consumer must take to implement such controls."[49]

F. Users Oppose Facebook's Additional Facial Recognition Techniques

111. Jared Bennett of Center for Public Integrity remarked on Facebook's "uniquely aggressive" opposition to any limits on its increasingly intrusive facial recognition technology. [50]

> In 2012, at a hearing of the Senate Judiciary Subcommittee on Privacy, Technology, and the Law, then-Chairman Al Franken (D-MN) asked Facebook's then-manager of privacy and public policy, Rob Sherman, to assure users the company wouldn't share its faceprint database with third parties. Sherman declined.

112. Facebook has still not clarified in 2018 which third parties have access to users' biometric data, and the purposes of disclosures.

113. WIRED Reporter Lily Hay Newman commented:[51]

---

[48] *See* Lily Hay Newman, *supra*.
[49] Facebook Consent Order.
[50] Jared Bennett, *Facebook: Your Face Belongs to Us* The Daily Beast, July. 31, 2017. https://www.thedailybeast.com/how-facebook-fights-to-stop-laws-on-facial-recognition.
[51] Lily Hay Newman, *supra*.

> Observers also note that limited face recognition applications for users doesn't necessarily mean that Facebook as a company isn't deriving a larger benefit from all the biometric face data it gathers. As a public company, if Facebook can find opportunities to monetize the data or harness it to fuel user growth, it will take them.

114. Mashable Reporter MJ Franklin also noted:[52]

> The in-app announcement was met with a great deal of skepticism. Fast Company pointed out that Facebook's announcement coincided with legal setbacks. According to Bloomberg, a federal judge recently ruled that the social network 'must face claims that it violated the privacy of millions of users by gathering and storing biometric data without their consent.

115. Consumers publicly voiced their distrust and discomfort with Facebook's business changes to facial recognition, many of them noting that Facebook never sought their affirmative express consent:

[52] MJ Franklin, *How to turn off Facebook's new face recognition features* Mashable, Feb. 28, 2018, https://mashable.com/2018/02/28/how-to-turn-off-facebook-face-recognition/.

G. No Information on the Disclosure of Facial Recognition Data to Third Parties and Their Downstream Uses

116. Facebook announced significant changes to the facial recognition setting without explaining how the additional biometric data obtained from users and non-users will be disclosed to and used by third parties.

117. Facebook remains vague and unclear about how it utilizes the vast biometric data collected from users and non-users, with the Tag Suggestions and its subsequent facial recognition techniques.

118. Facebook's privacy policy does not specifically address the implications of facial recognition data by third-party service providers and advertisers, despite the heightened sensitivities of biometric personal information.

119. Facebook's privacy policy on "Sharing with Third-Party Partners" claims that advertisers and analytics services only have access to "non-personally identifiable information."[53]

> We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you.

[53] Facebook, *Data Policy*, (Sep. 29, 2016) https://www.facebook.com/full_data_use_policy.

120. Facebook does explain how an identity-matched facial image is not personally identifiable information.

121. Facebook's definition of PII is limited and misleading: "information like name or email address that can by itself be used to contact you or identifies who you are."[54] Facebook does not consider the privacy implications of information that may not independently be personally identifiable but can be readily matched with other demographic segments and quasi-identifiers to pinpoint one person with sufficient accuracy.

> **Advertising, Measurement and Analytics Services (Non-Personally Identifiable Information Only).**
> We want our advertising to be as relevant and interesting as the other information you find on our Services. With this in mind, we use all of the information we have about you to show you relevant ads. We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you. For example, we may tell an advertiser how its ads performed, or how many people viewed their ads or installed an app after seeing an ad, or provide non-personally identifying demographic information (such as 25 year old female, in Madrid, who likes software engineering) to these partners to help them understand their audience or customers, but only after the advertiser has agreed to abide by our advertiser guidelines.
>
> Please review your advertising preferences to understand why you're seeing a particular ad on Facebook. You can adjust your ad preferences if you want to control and manage your ad experience on Facebook.

122. Facebook's Help Center claims that facial template data is stored as a "unique number."[55]

---

[54] *Id.*
[55] Facebook Help Center, *How does Facebook's face recognition work?* (2018), https://www.facebook.com/help/122175507864081.

> Our technology analyzes the pixels in photos and videos, such as your profile picture and photos and videos that you've been tagged in, to calculate a unique number, which we call a template.

123. From this definition, it is highly possible that Facebook may classify biometric templates as non-personally identifiable information that can be disclosed to third parties and advertisers. Facebook may consider facial recognition data to be sufficiently "de-identified" by the numerical scoring process, and overlook the privacy implications of giving third parties access to the data.

124. Facebook could also disclose biometric data to third parties by contending that the user gave consent. Given the current opt-out setting for facial recognition and the various misrepresentations made by Facebook to induce consumers into adopting privacy-invasive technologies, the FTC should investigate whether Facebook's "data-sharing programs with third parties" violate the 2011 Consent Order.

H. Facebook Fails to Establish that Application Developers, the Government, and Other Third Parties Will Not Be Able to Access Users' Biometric Data

125. The Facebook Platform makes a variety of personal data available to application developers and external websites.[56] Application developers obtain access to account information when they connect with an application.[57] Applications may also obtain users' friends' data,[58] and access connections between users who have both connected to an application.[59]

126. App developers have access to the Facebook graph API. It "presents a simple, consistent view of the Facebook social graph, uniformly representing objects in the graph (e.g., people, photos, events, and pages) and the connections between them (e.g., friend relationships, shared content, and photo tags)."[60] Developers may leverage this API within apps.

127. Websites implementing Facebook plugins can use the Graph API "to access the user's Facebook profile. . . to access the user's social graph, bring their friends directly to your site all in your own custom experience."[61]

128. To obtain personal data to develop applications, developers may only request the information that they need to operate their application. However, Facebook does not

[56] Facebook Platform Policies, Storing and Using Data You Receive From Us, https://developers.facebook.com/policy ("Platform Policies").
[57] *Id.* at ¶5.
[58] *Id.* at ¶4.
[59] *Id.* at ¶11.
[60] Facebook Developers, Graph API, https://developers.facebook.com/docs/reference/api.
[61] Facebook for Websites, Personalization, https://developers.facebook.com/docs/guides/web/#personalization.

define what is necessary, and the terms leave developers to determine what they need.[62]

129. Facebook maintains different standards for information provided to advertisers and information Facebook will use to target advertisements to users. Facebook may make use of underlying, non-profile user data. For example, while Facebook may not provide users' IP addresses directly to advertisers, Facebook Ads uses IP addresses to determine users' locations and target ads to those locations.[63]

130. Facebook does not always maintain control over how user data is used by advertisers. An advertiser was caught using profile pictures in singles dating service advertisements, and Facebook spokesperson Barry Schnitt announced that "the ads that spooked people were from rogue networks…"[64] Facebook claims that policing over 500,000 apps and advertisers is impracticable, as advertisers and rogue networks can choose not to disclose what they are actually doing with Facebook-provided user data.[65] Advertisers may cache Facebook user data indefinitely.

131. Facebook's published privacy policy states that the company may "disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law."[66] The U.S. Department of Justice ("DOJ") has stated that the "standard data production" from Facebook includes "photoprint," contact information, and Internet Protocol logs, while noting that "other data" is available and that Facebook is "often cooperative with emergency requests."[67]

132. The U.S. government has an interest in accessing the information present on Facebook and other social networking sites,[68] and law enforcement has used Facebook in pursuing investigations.[69] Training materials used by DOJ have suggested that law enforcement agents can use evidence gathered from social networks to "reveal personal communications; establish motives and personal relationships; provide location information; prove and disprove alibis; [and] establish crime or criminal enterprise," among other "instrumentalities or fruits of crime."[70]

---

[62] Platform Policies, *supra*, at ¶1.
[63] Reach and Targeting, *Reach Real People with Precise Targeting, at Location Targeting*, https://www.facebook.com/adsmarketing/index.php?sk=targeting_filters.
[64] Ethan Beard, *A New Data Model*, Facebook Developer's Blog, Apr. 21, 2010, https://developers.facebook.com/blog/post/378.
[65] Kim-Mai Cutler, *New data storage rules, permissions could rekindle Facebook privacy concerns*, Social Beat, Apr. 28, 2010, http://venturebeat.com/2010/04/21/facebook-privacynew-data-storage-rules.
[66] Facebook, Privacy Policy, https://www.facebook.com/policy.php.
[67] John Lynch & Jenny Ellickson, U.S. Dept. of Justice, Computer Crime and Intellectual Property Section, *Obtaining and Using Evidence from Social Networking Sites: Facebook, MySpace, Linkedln, and More*, Mar. 2010, at 17, http://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf.
[68] *Id.*
[69] *See, e.g.,* Julie Masis, *Is this Lawman your Facebook Friend?*, Boston Globe, Jan. 11, 2009, http://www.boston.com/news/local/articles/2009/01/11/is_this_lawman_your_facebook_friend .
[70] John Lynch & Jenny Ellickson, *supra*.

The same training materials include a screenshot of the picture "tagging" process[71] and makes reference to the one billion pictures being added every month.

I. Privacy Controls to Opt-Out of Facial Recognition Are Not Clear and Prominent

133. The 2011 FTC Consent Order requires that Facebook obtain affirmative express consent to override existing privacy settings. The Commission authoritatively expressed that Facebook must respect user consent by providing an affirmative opt-in choice for new business practices that implicate consumer privacy.[72]

> Part II of the proposed order requires Facebook to give its users a clear and prominent notice and obtain their affirmative express consent before sharing their previously-collected information with third parties in any way that materially exceeds the restrictions imposed by their privacy settings.

134. Consent must be meaningful and specific, and obtained from informed users. Cumbersome opt-out settings violate the high standard of compliance imposed by Consent Order.

135. Notwithstanding the clear requirements of the Consent Order, Facebook placed the burden on its users to opt-out of facial recognition. It has further misrepresented the simplicity of the opt-out choice as a "simple setting,"[73] toggled by a "single on/off control" when it announced changes to the facial recognition practice.

136. On December 19, 2017, Facebook's Director of Applied Machine Learning Joaquin Quiñonero Candela posted an announcement entitled, "Managing Your Identity on Facebook with Face Recognition Technology."

> You control whether Facebook can recognize you in photos and videos. Soon, you will begin to see a simple on/off switch instead of settings for individual features that use face recognition technology. We designed this as an on/off switch because people gave us feedback that they prefer a simpler control than having to decide for every single feature using face recognition technology. To learn more about all of these features, visit the Help Center or your account settings.

137. The "on/off switch" requires the user to navigate multiple Facebook settings to locate. Facebook did not operationalize opt-out with an intuitive and distinguishable setting.

138. On a phone, the user must open the Facebook app and tap on the overflow button (three-line icon). Then go to Settings > Privacy Shortcuts > More Settings > Face

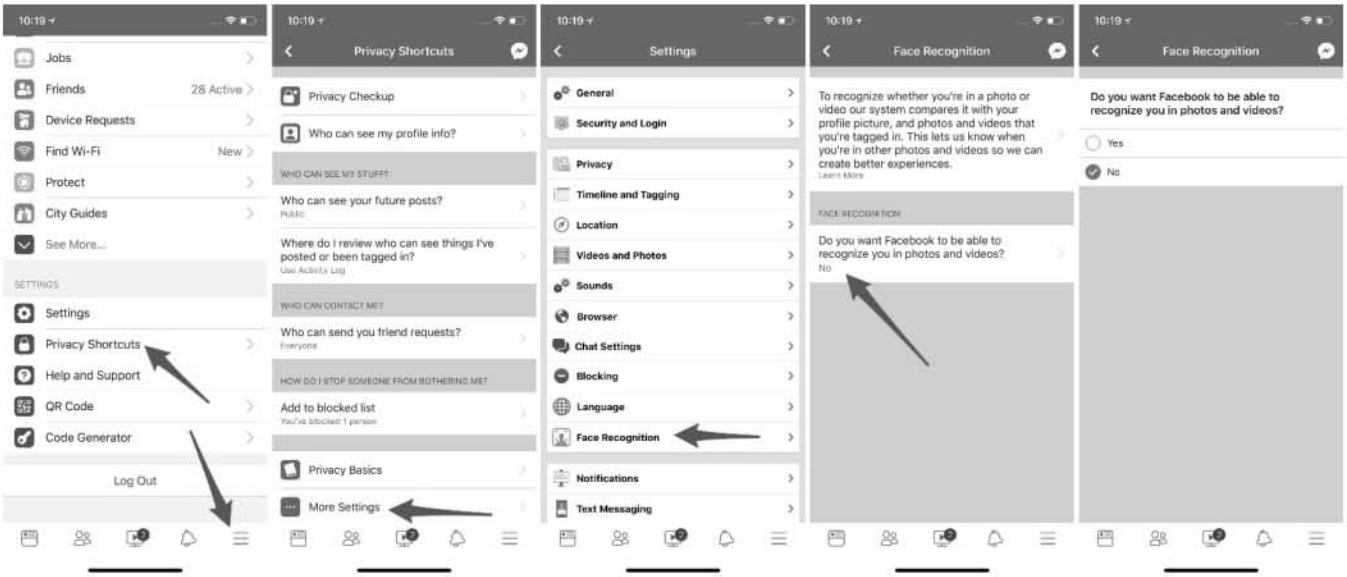
---

[71] *Id*. at 15.
[72] Facebook, Inc. Proposed Consent Order.
[73] Joaquin Quiñonero Candela, *Managing Your Identity on Facebook with Face Recognition Technology*, Facebook Newsroom, (Dec.19, 2017), https://newsroom.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/.

Recognition, then tap on the Face Recognition question. Finally, they can select No after this five-step process.

139. Ordinary consumers will face immense difficulty in locating the opt-out switch, just like they did in 2013 when Tag Suggestions were automatically turned on.

140. This indicates a violation of the Consent Order regarding affirmative consent as well as clear and prominent notice. The confusing setting invalidates affirmative consent by making the exercise of choice inaccessible for a majority of users. It also diminishes user awareness of the existence of this facial recognition setting.



J. Facebook is Pursuing the Commercialization of Biometric Data

141. Facebook economically benefits from the development of facial recognition techniques.

142. Facebook routinely makes misrepresentations to induce consumers to adopt wider and more pervasive uses of facial recognition technology. Therefore, the FTC must exercise the fullest extent of its legal authority to prohibit and limit these privacy-invasive technologies by enforcing the 2011 Consent Order.

i. Facebook's Facial Recognition Patents

143. In 2017, Facebook submitted four patent applications[74] on facial recognition techniques.

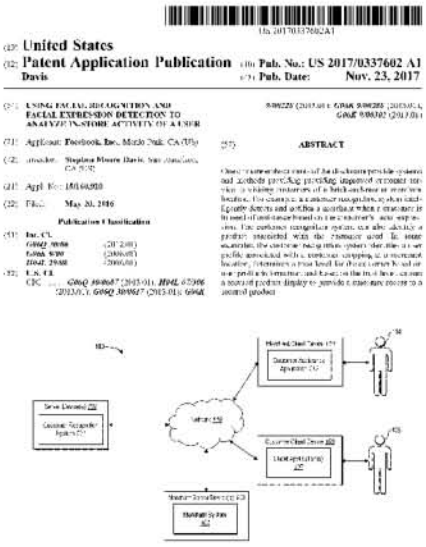
144. On March 9, 2017, Facebook submitted a patent application for "Facial Recognition Using Social Networking Information," which details a system that detects and tracks

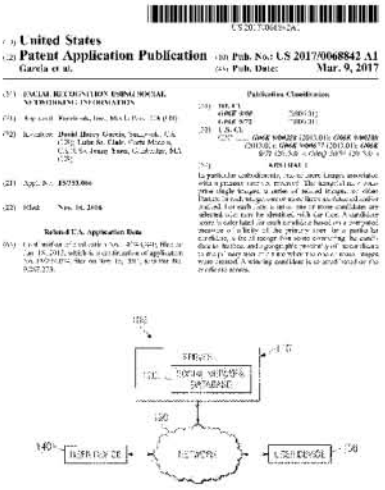
[74] USPTO Applicaton #: #20170337602; USPTO Applicaton #: #20170323299; USPTO Applicaton #: #20170140214; USPTO Applicaton #: #20170068842.

the exact geographic dimensions of a candidate's facial features to apply a template "score" that can be compared across various "faces in video, photos, or other media hosted on the social network"[75] for biometric matches.

145. On November 2017, Facebook filed two patents for "Facial Recognition Identification for In-Store Payment Transactions" and "Using Facial Recognition and Facial Expression Detection to Analyze In-Store Activity of a User."

146. The two applications detail a customer recognition system which "intelligently detects and notifies a merchant when a customer is in need of assistance based on the customer's facial expression. The customer recognition system can also identify a product associated with the customer need."





147. Facebook's patent applications attest to the company's primary commercial purpose in expanding its biometric data collection, and the pervasive uses of facial recognition technology that it envisions for the near future. The FTC must ensure that Facebook adheres to its obligations for user privacy as compelled by the 2011 Consent Order.

ii. Facebook's Annual Report to the Securities and Exchange Commission

148. Facebook's annual filing to the Securities and Exchange Commission ("SEC") for the 2017 fiscal year explicitly states that compliance with the FTC Consent Order and

[75] *Available at,* http://www.freshpatents.com/-dt20170309ptan20170068842.php; http://www.freshpatents.com/-dt20171109ptan20170323299.php.

modifying the company's practices to obtain affirmative express consent could "adversely affect financial results."[76]

149. On enforcement actions on the Consent Order, Facebook claimed:

> Affected users or government authorities could initiate legal or regulatory actions against us in connection with any security breaches or improper disclosure of data, which could cause us to incur significant expense and liability or result in orders or consent decrees forcing us to modify our business practices. Such incidents may also result in a decline in our active user base or engagement levels. Any of these events could have a material and adverse effect on our business, reputation, or financial results.

150. On modifying practices to obtain consent, Facebook claimed:

> [R]egulatory or legislative actions affecting the manner in which we display content to our users or obtain consent to various practices could adversely affect user growth and engagement. Such actions could affect the manner in which we provide our services or adversely affect our financial results.[77]

151. These financial disclosures expressly indicate that Facebook is structurally and economically incentivized to monetize greater data collection. Facebook admits that modifying its practices to obtain consent for various practices will detriment its user growth and "engagement," leading to negative financial results. The FTC must affirmatively enforce the Consent Order against Facebook to ensure that it fully complies with all the provisions of the settlement.

K. Facebook Has Consistently Failed to Ensure Compliance by App Developers

152. In 2009, Facebook operated a deceptive Verified Apps program which claimed that Facebook gives preferential treatment to Platform Applications whose security standards exceed expectations in Facebook's "detailed review process."

153. Facebook misrepresented to its users that Verified Apps will "offer extra assurances to help users identify applications they can trust -- applications that are secure, respectful and transparent, and have demonstrated commitment to compliance with Platform policies."[78]

154. However, an investigation by the Commission revealed that Facebook had misrepresented the heightened security of Verified Apps. The FTC detailed this

---

[76] Facebook, Annual Report, SEC File No., 001-35551, at 13, (2016), https://www.sec.gov/Archives/edgar/data/1326801/000132680117000007/fb-12312016x10k.htm.
[77] *Id.* at 16.
[78] Facebook, *Facebook Expands Power of Platform Across the Web and Around the World*, Press Release, July 23, 2008, https://newsroom.fb.com/news/2008/07/facebook-expands-power-of-platform-across-the-web-and-around-the-world/.

deceptive practice in the complaint that underlies the 2011 Consent Order against Facebook: [79]

> Contrary to the statements set forth … before it awarded the Verified Apps badge, Facebook took no steps to verify either the security of a Verified Application's website or the security the Application provided for the user information it collected, beyond such steps as it may have taken regarding any other Platform Application.

155. Unfortunately, recent revelations of Facebook's negligence in disclosing the personal data of 50 million American voters to Cambridge Analytica and various affiliates show that Facebook has not improved its verification of app developers in the post-FTC Consent Order era.

156. On March 20, 2018, a former Facebook Operations Manager from 2011 to 2012 Sandy Parakilas published an article entitled "I worked at Facebook. I know how Cambridge Analytica could have happened."[80]

> Critically, once the data passed from Facebook's servers to the developer, Facebook lost all insight into or control over how the data was used. To prevent abuse, Facebook created a set of platform policies that forbade certain kinds of activity, such as selling the data or passing it to an ad network or data broker such as Cambridge Analytica. However, Facebook had very few ways to discover abuse or act on it once discovered.

157. Parakilas details Facebook's routine indifference to apps that violated policies and the Terms of Service.

> Facebook had the following tools to deal with these cases: It could call the developer and demand answers; it could demand an audit of the developer's application and associated data storage, a right granted in the platform policies; it could ban the developer from the platform; it could sue the developer for breach of the policies, or it could do some combination of the above. During my 16 months at Facebook, I called many developers and demanded compliance, but I don't recall the company conducting a single audit of a developer where the company inspected the developer's data storage. Lawsuits and outright bans were also very rare. I believe the reason for lax enforcement was simple: Facebook didn't want to make the public aware of huge weaknesses in its data security.

---

[79] Fed. Trade Comm'n, Facebook, Inc., FTC File No. 092 3184 (2011) (Complaint), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf.

[80] Sandy Parakilas, *I worked at Facebook. I know how Cambridge Analytica could have happened* The Washington Post, Mar. 20, 2018, https://www.washingtonpost.com/opinions/i-worked-at-facebook-i-know-how-cambridge-analytica-could-have-happened/2018/03/20/edc7ef8a-2bc4-11e8-8ad6-fbc50284fce8_story.html.

158. Parakilas compares Facebook's disregard for data protection in 2012 to the 2018 Cambridge Analytica scandal, and concludes that compliance has not improved:

> Facebook will argue that things have changed since 2012 and that the company has much better processes in place now. If that were true, Cambridge Analytica would be small side note, a developer that Facebook shut down and sued out of existence in December 2015 when word first got out that it had violated Facebook's policies to acquire the data of millions. Instead, it appears Facebook used the same playbook that I saw in 2012. It took the developer's word rather than conducting an audit, and it ignored press reports about Cambridge Analytica using Facebook data in violation of its terms during the election.

159. On March 20, 2018, EPIC and a coalition of consumer organizations urged the FTC to reopen the investigation of Facebook, and to sanction the company's clear violations of the 2011 Consent Order.[81]

> "As the Facebook Order makes clear, Facebook must "get consumers' approval before it changes the way it shares their data," and must "obtain consumers' affirmative express consent before enacting changes that override their privacy preferences." The FTC also barred Facebook from "making misrepresentations about the privacy or security of consumers' personal information."
>
> Yet Facebook's business practices resulted in the disclosure of consumers' "names, education, work histories, birthdays, likes, locations, photos, relationship statuses, and religious and political affiliations" to Cambridge Analytica without their knowledge or consent. In 2014, Facebook acknowledged that it allowed app developers to access profile information on an app users' friends without the friends' knowledge or consent, stating that consumers "are often surprised when a friend shares their information with an app." Facebook's admission that it disclosed data to third parties without users' consent suggests a clear violation of the 2011 Facebook Order."

160. The FTC has an affirmative duty to undertake a review of substantial changes in Facebook's business practices that implicate user privacy and to ensure compliance with the Consent Order.

161. Facebook's change to the facial recognition setting was implemented without the affirmative express consent of users. This substantial change in business practice is a serious consent decree violation which the FTC must enjoin immediately. It is imperative that the Commission pursue an investigation to prohibit the unlawful proliferation of biometric data collection by Facebook and its unaccountable commercial counterparts.

---

[81] EPIC, *EPIC, Consumer Groups Urge FTC To Investigate Facebook* (Mar. 20, 2018), https://epic.org/2018/03/epic-consumer-groups-urge-ftc-.html. f

L. Facial Recognition is Illegal in Other Countries

162. Canada and Europe limit how companies can collect and store biometric data. The deployment of commercial facial recognition technology is widely considered an invasion of privacy rights in Canada and Europe.

163. The Privacy Commissioner's Office found Facebook "in contravention" of Canada's Personal Information Protection and Electronic Documents Act.[82]

164. The EU Article 29 Data Protection Working Party issued an opinion on developments in biometric technologies which states that consent must be obtained for the storage and use of biometric data. [83]

165. On October 15, 2012, Facebook disabled its tagging facial recognition practice for users in the European Union, following an investigation by the Irish Data Protection Commissioner.

166. In 2015, Facebook created a photo-sharing app called Moments which does not use facial recognition technology for Canadian and European users.

167. The BBC reported that Facebook Moments Product Manager Will Ruben stated that the phone is given a numerical representation of a face, "but that number is not stored anywhere on our servers, and it is only used to compare against the other photos on your phone."[84]

168. The Inquirer reported that a Facebook spokesperson said: "Facebook has notified this office of the Moments app and advised us that in the EU version of the Moments app they do not control or initiate the use of any feature recognition technology." [85]

169. Facebook is capable of developing alternative techniques that are less privacy-invasive. The photo sharing aspect of the social media network can be facilitated without the use of privacy-pervasive facial recognition technology, as it has been done for Canada and Europe.

170. The disparity of privacy protections afforded for the nationals and residents of the United States due to the lack of enforcement action against Facebook is unacceptable.

---

[82] Elizabeth Denham, Assistant Privacy Commissioner of Canada, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act* (July 16, 2009), http://priv.gc.ca/cfdc/2009/2009_008_0716_e.pdf.

[83] Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* (Apr. 27, 2012), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

[84] Leo Kelion, *Facebook Moments facial-recognition app launches in Europe* BBC News, May 10, 2016, http://www.bbc.com/news/technology-36256765.

[85] Carly Page, *Facebook launches facial recognition app in Europe, without facial recognition tech,* The Inquirer, May 11, 2016, https://www.theinquirer.net/inquirer/news/2457657/facebook-launches-face-recognition-app-in-europe-without-face-recognition-tech.

171. The FTC is the primary privacy regulator in the United States. The Commission must enforce the Consent Order to compel Facebook to modify its business practice to comply with strict privacy protections.

V. Prior Consumer Complaints to the FTC Regarding Facebook's Facial Recognition

172. EPIC has previously urged the Commission to prohibit Facebook's facial recognition techniques on multiple occasions.

173. In June 2011, EPIC and a coalition of consumer organizations filed a complaint with the FTC alleging that Facebook's covert deployment of its facial recognition technology was unfair and deceptive.[86] EPIC stated that Facebook's "Tag Suggestions" technique, "converts the photos uploaded by Facebook users into an image identification system under the sole control of Facebook. This has occurred without the knowledge or consent of Facebook users and without adequate consideration of the risks to Facebook users."[87] EPIC warned that "unless the Commission acts promptly, Facebook will routinely automate facial identification and eliminate any pretense of user control over the use of their own images for online identification."[88] EPIC emphasized that the Commission's "failure to act on pending consumer complaints concerning Facebook's unfair and deceptive trade practices may have contributed to Facebook's decision to deploy facial recognition."[89]

174. In December 2011, EPIC urged the Commission to strengthen its proposed settlement with Facebook by requiring it to "cease creating facial recognition profiles without users' affirmative consent."[90] EPIC contended that while the Order's broad prohibition on privacy misrepresentations already covered Facebook's deceptive use of facial recognition, the Order should have been amended to proscribe the practice explicitly.[91]

175. In January, 2012, EPIC submitted extensive comments in response to the FTC's workshop "Face Facts: A Forum on Facial Recognition Technology."[92] EPIC again emphasized that Facebook's facial recognition practice "entirely fails at informing users how their photo data will be used or to provide any meaningful consent for use," as required by the Order. EPIC advised the Commission that, "Commercial actors should not deploy facial techniques until adequate safeguards are established. As such

---

[86] In the Matter of Facebook, Inc. and the Facial Identification of Users (EPIC Complaint, Request for Investigation, Injunction, and Other Relief) (June 10, 2011), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf.
[87] *Id.*
[88] *Id.*
[89] *Id.*
[90] *Comments of EPIC*, In the Matter of Facebook, Inc., FTC File No. 092 3184 (Dec. 27, 2011), https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf.
[91] *Id.*
[92] *Comments of EPIC*, "Face Facts: A Forum on Facial Recognition," Project No. P115406, (Jan. 31, 2012), https://epic.org/privacy/facerecognition/EPIC-Face-Facts-Comments.pdf.

safeguards have not yet been established, EPIC would recommend a moratorium on the commercial deployment of facial recognition techniques."[93]

VI. The Importance of Enforcing Consent Orders for Consumer Privacy

176. The effectiveness of the FTC depends upon the agency's willingness to enforce the legal judgments it obtains. However, the FTC routinely fails to enforce its consent orders, which promotes industry disregard for the FTC. Companies under consent decree have no incentive to protect consumer data if they do not anticipate the FTC to hold them accountable when they violate consent decrees.

177. EPIC and other consumer organizations have routinely called attention to the numerous changes Facebook has made to its privacy settings without obtaining users' affirmative consent, in violation of the terms of its FTC consent decree.[94]

178. In 2011, Facebook entered into a 20-year consent order with the FTC in which it agreed that it "shall not misrepresent … the extent to which it maintains the privacy or security of covered information," and would provide disclosure separate from its privacy policy.[95]

it agreed that it "shall not misrepresent … the extent to which it maintains the privacy or security of covered information," and would provide disclosure separate from its privacy policy.[96]

179. On December 17, 2009, EPIC and 14 consumer and privacy organizations filed a Complaint with the FTC concerning Facebook's unfair and deceptive trade practices. The complaint cited widespread opposition from Facebook users, Senators, bloggers, and news organizations.[97]

180. EPIC's Complaint noted that "Facebook's changes to users' privacy settings disclose personal information to the public that was previously restricted. Facebook's changes to users' privacy settings also disclose personal information to third parties that was previously not available. These changes violate user expectations, diminish user privacy, and contradict Facebook's own representations."[98]

---

[93] *Id.*
[94] EPIC, *In the Matter of Facebook Inc: Complaint, Request for Investigation, Injunction, and Other Relief* (Dec. 17, 2009), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf; ("EPIC 2009 Facebook Complaint").EPIC *In the Matter of Facebook Inc: Complaint, Request for Investigation, Injunction, and Other Relief* (May 5, 2010),. ("EPIC Supplemental Facebook Complaint"), https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf.
[95] Facebook Consent Order.
[96] *Id.*
[97] EPIC 2009 Facebook Complaint.
[98] *Id.*

181. On January 14, 2010, EPIC filed a second Complaint with the Commission concerning Facebook's unfair and deceptive trade practices.[99]

182. EPIC's amended Complaint observed that Facebook's business practices "violate user expectations, diminish user privacy, and contradict Facebook's own representations."[100]

183. In a subsequent letter to Congress, EPIC urged the Members of the House and Senate oversight committees to pay careful attention to a new complaint that the consumer and privacy organizations had presented to the Federal Trade Commission regarding Facebook and change to user profile information and the disclosure of user data to third parties without consent.[101] The complaint alleged that these actions "violate user expectations, diminish user privacy, and contradict Facebook's own representations." EPIC noted that the complaint alleged unfair and deceptive trade practices that "subject to investigation and prosecution under Section 5 of the Federal Trade Commission Act."[102]

184. The letter cited numerous other complaints concerning regarding Facebook brought to the attention of the FTC in which the Commission failed to act. The EPIC letter warned:

> In the past, the Federal Trade Commission has taken decisive steps to safeguard consumer privacy. These decisions help spur innovation and competition, reduce risk to consumers, and promote trust and confidence in new business services. But the current FTC appears reluctant to take similar steps on behalf of American consumers.

185. To date, the FTC has failed to take any action with respect to Facebook's changes in biometric privacy practices.

186. The Commission's failure to act on these prior complaints may have contributed to Facebook's decision to deploy face recognition technology as it did.

187. Companies and consumer organizations may disagree as to whether a significant change in business practices violates a consent order. That is a decision ultimately for the Commission. But it is incumbent upon the FTC to develop a process that ensures a reasoned decision, subject to public review. At present, there is no meaningful public process to ensure compliance with FTC consent orders.

VI. Legal Analysis

---

[99] *Id.*
[100] *Id.*
[101] Letter to Senator Rockefeller, et al from EPIC Executive Director Marc Rotenberg (May 5, 2010), http://epic.org/privacy/facebook/EPIC_FB_FTC_Complaint_Letter.pdf.
[102] *Id.*

188. The 2011 FTC Consent Order arises from a series of complaints filed by EPIC and other consumer privacy organizations from 2009 to 2011concerning material changes to privacy settings made by Facebook.

189. Pursuant to EPIC's requests for investigation, the Commission filed an eight-count complaint against Facebook for unfair and deceptive practices in contravention of Section 5 of the Federal Trade Commission Act.

190. On November 29, 2011, the FTC published a press release announcing that Facebook settled charges with the Commission. The FTC enumerated a list of prohibited practices under the proposed settlement:

"Specifically, under the proposed settlement, Facebook is:

- "barred from making misrepresentations about the privacy or security of consumers' personal information;
- "required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences;
- "required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;
- "required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers' information; and
- "required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected."

191. The Commission has a non-discretionary obligation to enforce a final order.

192. To date, the FTC has failed to take any action with respect to Facebook's changes in biometric privacy practices. Critically, the Commission has not filed a lawsuit pursuant to, the Federal Trade Commission Act which states that the FTC "shall" obtain injunctive relief and recover civil penalties against companies that violate consent orders. 15 U.S.C. § 45(l).

193. The FTC has exclusive authority over the enforcement of its consent orders. The enforcement provision of the FTC Act, Section 5(l), makes clear that the agency action is not discretionary; a violating party "shall forfeit" a penalty and be subject to an enforcement action.

194. The FTC is charged with performing a "discrete agency action." A "discrete agency action" is a "final agency action" under the Administrative Procedure Act. *In re Aiken County*, 645 F.3d 428, 437 (D.C. Cir. 2011). "Agency action unlawfully withheld" is a defined as "discrete agency action that [the agency] is required to take." *Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 64 (2004).

195. Agency action is the "whole or part of an agency rule order, license, sanction, relief, or the equivalent or denial thereof, or failure to act." 5 U.S.C. § 551 (13). Agency action, including a "failure to act" is subject to judicial review. *Amador County, Cal. v. Salazar*, 640 F.3d 373, 383 (D.C. Cir. 2011)

196. Here the FTC unlawfully withheld such an action – namely commencing a civil action for violation of its consent order, and has failed to perform by not enforcing its 2012 Consent Order against Facebook.

197. EPIC may "compel agency action unlawfully withheld" pursuant to the Administrative Procedure Act. 5 U.S.C. § 706(1).

VII. Prayer for Investigation and Relief

198. Facebook's actions injure users throughout the United States by invading their privacy; allowing for disclosure and use of information in ways and for purposes other than those consented to or relied upon by such users; causing them to believe falsely that they have full control over the use of their information; and undermining the ability of users to avail themselves of the privacy protections promised by the company.

199. The FTC Act empowers and directs the FTC to investigate business practices, including data collection practices that constitute consumer harm.[103]

200. Petitioners request that the Commission investigate Facebook, enjoin the deployment of additional facial recognition techniques as a violation of the 2011 Consent Order, and require Facebook to modify its biometric data practices to protect the privacy of Facebook users and non-users. Specifically, Petitioners ask the Commission to:

    a. Require Facebook to suspend immediately any form of Facebook-initiated automated facial scanning or other forms of biometric identification of Facebook users based on Facebook's internal database of facial images.

    b. Delete all facial images, facial templates, and biometric identifiers wrongfully obtained

    c. Require Facebook to not misrepresent in any manner, expressly or by implication the extent to which Facebook maintains and protects the security, privacy, confidentiality, and integrity of any consumer information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects

[103] 15 U.S.C. § 45.

and uses consumer information (2) the extent to which consumers may exercise control over the collection, use, or disclosure of consumer information.

d. Require Facebook to expressly categorize the types of user information it collects, and to clarify which type of third party gets access to which categories of user information, and for what purpose.

e. Require Facebook to alert its users on the privacy implications of the services of Facebook and its subsidiaries which collect, store, and disclose biometric data. Prohibit Facebook from inducing users into embracing pervasive augmentations of facial recognition technology with announcements that misrepresent the commercial purposes for which Facebook collects users' facial templates.

f. Require that Facebook, prior to any new or additional disclosure by Facebook of a user's identified information to any third party, that: 1) is a change from stated sharing practices in effect at the time respondent collected such information, and 2) results from any change, addition, or enhancement to a product or service by respondent, in or affecting commerce, Facebook shall: A. clearly and prominently disclose: (1) that the user's information will be disclosed to one or more third parties, (2) the identity or specific categories of such third parties, and (3) the purpose(s) for Facebook's sharing; and B. Obtain express affirmative consent from the user to such sharing.

g. Audit and ensure that Facebook maintains a comprehensive privacy program, as required by the 2011 Consent Order, that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the security, privacy, confidentiality, and integrity of consumer information. Such program should include:

    1. the identification of reasonably-foreseeable, material risks, both internal and external, that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of consumer information or in unauthorized administrative control of Facebook, and an assessment of the sufficiency of any safeguards in place to control these risks.

    2. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

h. Require Facebook to establish appropriate security and privacy safeguards for biometric data practices, such as implementing an opt-in control for users, notifying users of business changes to encourage the exercise of informed choice, and limiting the disclosure of facial template data to third parties.

i. Seek appropriate injunctive and compensatory relief.

201. EPIC, and the consumer organizations listed above, reserve the right to amend this complaint and to bring other relevant matters to the attention of the Commission.

Respectfully submitted,

/s/ *Marc Rotenberg*
Marc Rotenberg
President EPIC

/s/ *Jeramie Scott*
Jeramie Scott
EPIC National Security Counsel
Coordinator, Privacy Coalition

/s/ *Sam Lester*
Sam Lester
EPIC Consumer Privacy Counsel

/s/ *Sunny Kang*
Sunny Kang
EPIC International Consumer Counsel

Electronic Privacy Information Center
Campaign for a Commercial Free Childhood
Center for Digital Democracy
Constitutional Alliance
Consumer Action
Consumer Federation of America
Consumer Watchdog
Cyber Privacy Project
Defending Rights & Dissent
Government Accountability Project
Patient Privacy Rights
Privacy Rights Clearinghouse
Southern Poverty Law Center
U.S. Public Interest Research Group

April 6, 2018

FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	)
	)
WhatsApp, Inc.	)
	)
	)

Complaint, Request for Investigation, Injunction, and Other Relief

Submitted by

The Electronic Privacy Information Center

and

The Center for Digital Democracy

I. Introduction

1. This complaint concerns the impact on consumer privacy of the proposed acquisition of WhatsApp, Inc. by Facebook, Inc. As set forth in detail below, WhatsApp built a user base based on its commitment not to collect user data for advertising revenue. Acting in reliance on WhatsApp representations, Internet users provided detailed personal information to the company including private text to close friends. Facebook routinely makes use of user information for advertising purposes and has made clear that it intends to incorporate the data of Whats App users into the user profiling business model. The proposed acquisition will therefore violate WhatsApp users' understanding of their exposure to online advertising and constitutes an unfair and deceptive trade practice, subject to investigation by the Federal Trade Commission.

II. Parties

2. The Electronic Privacy Information Center ("EPIC") is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FTC. EPIC has a particular interest in protecting consumer privacy, and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[1] EPIC's 2010 complaint concerning

[1] *See, e.g.*, Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm'r Christine

Google Buzz provided the basis for the Commission's investigation and October 24, 2011 subsequent settlement concerning the social networking service.[2] In that case, the Commission found that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz]."[3] The Commission's settlement with Facebook also followed from a Complaint filed by EPIC and a coalition of privacy and civil liberties organization in December 2009 and a Supplemental Complaint filed by EPIC in February 2010.[4] EPIC has previously urged the Commission to investigate businesses that make misleading representations as to record destruction practices. In 2008, EPIC notified the Commission that AskEraser falsely represented that search queries would be deleted when in fact they were retained by the company and made available to law enforcement agencies.[5]

3. The Center for Digital Democracy (CDD) is a not-for-profit DC-based organization focused on protecting consumers in the digital marketplace.[6] During the 1990's (and then operating as the Center for Media Education) its work to protect privacy on the Internet led to the passage of the Children's Online Protection Act (COPPA) by Congress in 1998.[7] CDD's advocacy on the Google-Doubleclick merger played a major role in the FTC's decision to address privacy concerns arising from online behavioral advertising.[8] Through a series of complaints filed at the commission, CDD has brought attention to privacy concerns with mobile devices, real-time tracking and targeting platforms, social

---

Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., *FTC* File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief) , http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[2] Press Release, Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://ftc.gov/opa/2011/03/google.shtm ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched.").

[3] *Id.*

[4] In the Matter of Facebook, Inc., (2009) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf [hereinafter EPIC 2009 Facebook Complaint]; In the Matter of Facebook, Inc., (2010) (EPIC Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief), https://*epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf* [hereinafter EPIC 2009 Facebook Supplement]; In the Matter of Facebook, Inc., (2010) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief) , https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf [hereinafter EPIC 2010 Facebook Complaint].

[5] EPIC: Does AskEraser Really Erase?, https://epic.org/privacy/ask/

[6] Ctr. for Digital Democracy, *About CDD*, http://www.democraticmedia.org/about-cdd (last accessed Mar. 6, 2014).

[7] Katherine C. Montgomery, *Generation Digital*, MIT PRESS, http://mitpress.mit.edu/books/generation-digital (last accessed Mar. 6, 2014).

[8] Louise Story, *F.T.C. Approves Doubleclick Deal*, N.Y. TIMES, Dec. 21, 2007, *available at* http://www.nytimes.com/2007/12/21/business/21adco.html.

media, and from the databroker industry.[9] CDD's recent four-year campaign to ensure that COPPA was effectively implemented across all major platforms and applications resulted in the FTC's December 2012 decision to strengthen its rules on children's privacy.[10]

4. WhatsApp, Inc. is an American incorporated in Delaware.[11] WhatsApp, Inc.'s primary place of business is 650 Castro Street, Suite 120-219, Mountain View, CA 94041.[12] WhatsApp, Inc. is the developer of WhatsApp, a subscription-based Small Message Service (SMS) application for mobile phones.[13] WhatsApp, Inc. was formed in 2009. The company currently processes over 10 billion messages per day from approximately 450 million active users.[14]

III. Factual Background

A. WhatsApp's Privacy Policies and Official Blog Posts Reflect a Strong Commitment to User Privacy

5. According to WhatsApp's privacy policy, last updated in July 2012, WhatsApp "does not collect names, emails, addresses or other contact information from its users' mobile address book or contact lists" other than mobile phone numbers.[15]

6. The mobile application's association of a phone number with a user's name "occurs dynamically on the mobile device itself and not on WhatsApp's servers and is not transmitted to WhatsApp."[16]

7. The only messages stored on WhatsApp servers are "undelivered" messages whose recipients have not logged into WhatsApp to retrieve messages. These are automatically deleted after 30 days.[17]

8. "The contents of messages that have ben delivered by the WhatsApp Service" are not copied, kept, or archived by WhatsApp in the normal course of business."[18]

---

[9] Rimma Katz, *Center for Digital Democracy asks FTC to investigate mobile data targeting*, MOBILE MARKETER, Apr. 9, 2010, *available at* http://www.mobilemarketer.com/cms/news/legal-privacy/5927.html.
[10] Press Release, Federal Trade Comm'n, FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Childrens Online Privacy Protection Rule (Dec. 19, 2012), http://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.
[11] California Secretary of State Business Entity Detail, http://kepler.sos.ca.gov/
[12] *Id*.
[13] Brian X. Chen and Vindu Goel, *Founders of an Anti-Facebook Are Won Over,* N.Y. TIMES, Feb. 21, 2014, http://nytimes.com/2014/02/21/technology/founders-of-an-anti-facebook-are-won-over.html.
[14] *Id*.
[15] WhatsApp Privacy Policy, http://www.whatsapp.com/legal/#Privacy
[16] *Id.*
[17] *Id*.
[18] *Id.*

9. WhatsApp's privacy policy states, "We do not use your mobile phone number or other Personally Identifiable Information to send commercial or marketing messages without your consent or except as part of a specific program or feature for which you will have the ability to opt-in or opt-out."[19]

10. On November 19, 2009, founder Jan Koum posted to the WhatsApp official Blog, **"**So first of all, let's set the record straight. We have not, we do not and we will not **ever** sell your personal information to anyone. Period. End of story. Hopefully this clears things up."[20]

11. On June 18, 2012, Koum posted to the WhatsApp Blog:

> At every company that sells ads, a significant portion of their engineering team spends their day tuning data mining, writing better code to collect all your personal data, upgrading the servers that hold all the data and making sure it's all being logged and collated and sliced and packaged and shipped out… And at the end of the day the result of it all is a slightly different advertising banner in your browser or on your mobile screen. … At WhatsApp, our engineers spend all their time fixing bugs, adding new features and ironing out all the little intricacies in our task of bringing rich, affordable, reliable messaging to every phone in the world. That's our product and that's our passion. Your data isn't even in the picture. We are simply not interested in any of it.[21]

12. On February 19, 2014, Koum posted to the WhatsApp Blog:

> Here's what will change for you, our users: nothing. WhatsApp will remain autonomous and operate independently. You can continue to enjoy the service for a nominal fee. You can continue to use WhatsApp no matter where in the world you are, or what smartphone you're using. And you can still count on absolutely no ads interrupting your communication. There would have been no partnership between our two companies if we had to compromise on the core principles that will always define our company, our vision and our product.[22]

---

[19] *Id*.
[20] WhatsApp Blog, *Just Wanted to Say a Few Things,* https://blog.whatsapp.com/index.php/2009/11/a-few-things/ (Nov. 9, 2009).
[21] WhatsApp Blog, *Why We Don't Sell Ads*, http://blog.whatsapp.com/index.php/2012/06/why-we-dont-sell-ads/ (Jun. 18, 2012).
[22] WhatsApp Blog, *Facebook*, http://blog.whatsapp.com/index.php/2014/02/facebook/ (Feb. 19, 2014).

13. Asked if the US government has attempted to access WhatsApp servers, Koum said, "People need to differentiate us from companies like Yahoo! and Facebook that collect your data and have it sitting on their servers. We want to know as little about our users as possible. We don't know your name, your gender… We designed our system to be as anonymous as possible. We're not advertisement-driven so we don't need personal databases."[23]

B. WhatsApp's Business Practices Affect Millions of Consumers

14. On August 23, 2012, WhatsApp processed ten billion user messages.[24]

15. On June 13, 2013, processed 27 billion user messages.[25]

16. As of December 2013, WhatsApp claimed that 400 million active users use the service each month.[26]

17. By the time the Facebook acquisition was announced at the end of February 2014, WhatsApp was processing 50 billion messages per day from 450 million monthly users.[27]

C. Facebook's Messaging Service Regularly Collects And Stores Virtually All Available User Data

18. When Facebook revamped its messaging system in November 2010, it automatically opted all users into the new messaging system.[28]

19. Facebook's new messaging system initially disabled users' ability to delete individual messages. [29]

20. Without user consent, the new messaging system also pulled data from Facebook's social graph to prioritize messages from certain users. [30]

---

[23] *Id*.
[24] Twitter, https://twitter.com/WhatsApp/status/238680463139565568 ("new daily record: 4B inbound, 6B outbound = 10B total messages a day! #freebsd #erlang") (last accessed Mar. 5, 2014).
[25] Twitter, https://twitter.com/WhatsApp/status/344966710241161216 (last accessed Mar. 5, 2014).
[26] WhatsApp Blog, http://blog.whatsapp.com/index.php/2013/12/400-million-stories/?lang=de
[27] Kristin Burnham, *Facebook's WhatsApp Buy: 10 Staggering Stats*, InformationWeek (Feb. 21, 2014), http://www.informationweek.com/software/social/facebooks-whatsapp-buy-10-staggering-stats-/d/d-id/1113927.
[28] Joel Seligstein, *See the Messages That Matter*, Facebook Blog, Nov. 15, 2011, https://www.facebook.com/notes/facebook/see-the-messages-that-matter/452288242130.
[29] Jan Jezabek, *Steps Toward the New Messaging System*, Facebook Blog, Nov. 2, 2011, https://developers.facebook.com/blog/post/591/
[30] Alex Wawro, *Facebook Messages: Our First Look,* PCWORLD, Nov. 15, 2010, http://www.techhive.com/article/210709/fbmessages_video1.html

21. Even when users delete a message, it continues to be stored on Facebook's servers.[31]

22. Even when a user chooses not to send a message, Facebook still tracks what the user wrote.[32]

D. Facebook Routinely Incorporates Data from Companies It Has Acquired

23. Facebook has regularly collected user data from companies it acquires.

24. For example, when Facebook purchased Instagram in 2012, Instagram users were not subjected to advertisements based on the content they uploaded to the site.[33]

25. Like WhatsApp, Instagram's Terms of Service included a provision that in the event of acquisition, users' "information such as name and email address, User Content and any other information collected through the Service may be among the items sold or transferred."[34]

26. After the acquisition, Facebook did in fact access Instagram users' data and changed the Instagram Terms of Service to reflect this change. [35]

E. Many WhatsApp Users Object to the Facebook Acquisition

27. Aliya Abbas, a Delhi-based mediaperson, said, "I started using WhatsApp five months ago. If it gets integrated with Facebook, I will uninstall [WhatsApp]. And I think others will do the same if this happens. WhatsApp is popular because of its

---

[31] Zack Whittaker, *Facebook Does Not Erase User-Deleted Content*, ZD NET, Apr. 28, 2010, http://www.zdnet.com/blog/igeneration/facebook-does-not-erase-user-deleted-content/4808; Miranda Miller, *Your Facebook Data File: Everything You Never Wanted Anyone to Know*, Search Engine Watch, Oct. 3, 2011, http://searchenginewatch.com/article/2114059/Your-Facebook-Data-File-Everything-You-Never-Wanted-Anyone-to-Know.

[32] Jennifer Golbeck, *On Second Thought… Facebook Wants to Know Why You Didn't Publish that Status Update You Started Writing*, SLATE, Dec. 13, 2013, http://www.slate.com/articles/technology/future_tense/2013/12/facebook_self_censorship_what_happens_to_the_posts_you_don_t_publish.html

[33] Craig Timberg, *Instagram outrage reveals a powerful but unaware Web community*, WASH. POST, Dec. 21, 2012, http://www.washingtonpost.com/business/technology/instagram-outrage-reveals-a-powerful-but-unaware-web-community/2012/12/21/b387e828-4b7a-11e2-b709-667035ff9029_story.html.

[34] *Id.*

[35] Hayley Tsukayama, *Instagram reminds users of privacy policy change*, WASH. POST, Jan. 16, 2013, http://www.washingtonpost.com/business/technology/instagram-reminds-users-of-privacy-policy-change/2013/01/16/124a8712-5fee-11e2-9940-6fc488f3fecd_story.html

privacy, and I don't think users will like the idea of advertisements popping up in the middle of a conversation."[36]

28. Columnist Carly Page wrote, "I'm a user of Whatsapp, and of course Facebook's ridiculously expensive acquisition of the firm has got me concerned about my privacy, especially the fact that the social network likely now has access to my mobile phone number."[37]

29. Journalist Tali Arbel wrote, "WhatsApp is my respite from Facebook. For me, the world's largest social network has become a junkyard of updates from people I don't really know and ads for products I don't care about. It's all about people jostling for publicity and craving approval, seeking likes and comments from near-strangers. But WhatsApp is the best stand-in for a conversation you have over dinner with people you love. It's intimate. It's personal. I rely on it. […] Facebook says it won't run ads on WhatsApp. But I'm afraid they won't be able to help themselves. With all those food pictures, won't Facebook figure I want to see ads for restaurants and cookware? And will Facebook urge my 'friends' to connect with me on WhatsApp? Facebook has done something similar with Instagram, the photo-sharing app it has owned since 2012."[38]

30. Corley Paige, a product developer from Austin, Texas, wrote, "I suddenly want to delete my Whatsapp. Hello Viber."[39]

31. Twitter user Tara Aghdashloo wrote, "Facebook is like an evil parent that keeps finding the new hiding place for your diary."[40]

32. User @tabandchord posted to Twitter, "Facebook + WhatsApp = The Ultimate Spying Machine #facebook #WhatsApp."[41]

33. Some users of both WhatsApp and Facebook created a Facebook Page titled "Please Don't Ruin WhatsApp." Under the designation "Community description,"

---

[36] Nitin Sreedhar, *Status update: WhatsApp now a chapter in Facebook,* BUSINESS STANDARD, Feb. 24, 2014, http://www.business-standard.com/article/technology/status-update-whatsapp-now-a-chapter-in-facebook-114022300669_1.html.
[37] Carly Page, *Facebook's Whatsapp buy is a privacy nightmare for users, but it makes sense for the social network*, THE INQUIRER, Feb. 20, 2014, http://www.theinquirer.net/inquirer/opinion/2329985/facebooks-whatsapp-buyout-is-a-privacy-nightmare-for-users-but-it-makes-sense-for-the-social-network.
[38] Tali Arbel, *My Love Affair With WhatsApp: Does It Have to End?*, WASH. TIMES, Feb. 20, 2104, http://www.washingtontimes.com/news/2014/feb/20/my-love-affair-with-whatsapp-does-it-have-to-end.
[39] Jessica Guynn, *Users threaten to delete WhatsApp now that Facebook is buying it,* LOS ANGELES TIMES, Feb. 19, 2014, http://www.latimes.com/business/technology/la-fi-tn-users-threaten-to-delete-whatsapp-20140219,0,4153795.story#axzz2v7TZZFCR.
[40] Twitter, https://twitter.com/taraaghdashloo/status/436272358312378371 (last accessed Mar. 5, 2014).
[41] Twitter, twitter.com/tabandchord

the page creators posted, "Hey Facebook: Please don't ruin WhatsApp and make all of our message go through Facebook Messenger." [42]

F. Industry Experts Warn that the Merger Will Diminish User Privacy

34. Industry experts object to the Facebook acquisition because it allows Facebook access to the repository of mobile phone numbers that WhatsApp has collected.

35. Wim Nauwelaerts, a lawyer specializing in EU data protection law at Hunton & Williams, LLP in Brussels, told *Bloomberg*, "Facebook is not only buying a popular messaging app, it is also acquiring the addresses and telephone numbers of 450 million users worldwide. […] Many of these users are already signed up to Facebook, so through this deal Facebook will be able to build complete profiles on users."[43]

36. St. John Deakins, the head of the online identity monitoring application Citizenme, said, "Facebook already has a very broad copyright license on people's content and already shares your data with many other services. Now with Facebook buying Whatsapp, this could see more and more private information becoming part of Facebook's database. From a personal data standpoint, this is extremely worrying."[44]

37. Tim Grossman, a senior branding consultant at Brand Union, wrote in *The Guardian*:

> "One of the reasons why so many millions have flocked to WhatsApp is the added level of privacy the brand provides. In a world where your every word echoes endlessly across the internet it was a communication channel where sharing could take place on a more contained level. However, much like Google's acquisition of Nest and Facebook's of Instagram, with this purchase consumers are suddenly associated with, and have their information accessible by a brand that they didn't buy into. It's this intrusion that can make it feel uncomfortable, as both you and your data are seized without your say-so."[45]

---

[42] Facebook, *Please Don't Ruin WhatsApp*, https://www.facebook.com/dontruinwhatsapp

[43] Stephanie Bodoni, *Facebook WhatsApp Deal Risks Sparking Privacy Probes Across EU*, BLOOMBERG, Feb. 25, 2014, http:// bloomberg.com/news/2014-02-25/facebook-whatsapp-deal-risks-sparking-privacy-probes-across-eu.html.

[44] Samuel Gibbs, *Six Alternatives to WhatsApp Now That Facbook Owns It*, THE GUARDIAN, Feb. 20, 2014, http://www.theguardian.com/technology/2014/feb/20/six-alternatives-whatsapp-facebook.

[45] Tim Gosman, *Why WhatsApp is a worthy addition to the Facebook fold*, THE GUARDIAN, http://www.theguardian.com/media-network/partner-zone-brand-union/facebook-acquisition-whatsapp-damage-brand-privacy.

G. Facebook's Acquisition of WhatsApp Implicates Safe Harbor Compliance

38. The Commission has previously issued an Order and Settlement Agreement with Facebook, following an investigation into whether "Facebook deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public."[46]

39. In addition to requiring Facebook to give users "clear and prominent notice" and obtain "their express consent before sharing their information beyond their privacy settings," and to maintain "a comprehensive privacy program to protect consumers' information," the Order also prohibited Facebook from misrepresenting the extent to which it participates in the US-EU Safe Harbor program.[47]

40. The Safe Harbor Framework is an industry-developed self-regulatory approach to privacy compliance.[48] Coordinated by the Department of Commerce, the Safe Harbor program allows firms to self-certify privacy policies in lieu of establishing adequate privacy protections in the United States that regulate business practice. The Safe Harbor arrangements developed in response to the European Union Data Directive, a comprehensive legal framework that established essential privacy safeguards for consumers across the European Union.[49]

41. The Federal Trade Commission has been tasked with penalizing US firms that incorrectly claim current Safe Harbor certification.[50]

42. Currently, Facebook represents that it complies with the requirements of Safe Harbor program.[51]

H. European Data Protection Authorities Have Already Begun Investigations

43. Jacob Kohnstamm, the Dutch data protection Commissioner, has begun an investigation into data protection issues related to Facebook's purchase of

---

[46] *In the Matter of Facebook, Inc., a corporation; FTC File No. 092 3184*, FTC.gov (Dec. 30, 2011), http://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.
[47] *Id*.
[48] U.S. Dep't of Commerce, Safe Harbor Privacy Principles, http://export.gov/safeharbor/eu/eg_main_018475.asp (last updated Jan. 30, 2009).
[49] Directive 95/46/EC of the European Parliament and of the Council of Oct. 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[50] Fed. Trade Comm'n, Bureau of Consumer Protection Business Center, *US-E.U. Safe Harbor Framework*, http://www.business.ftc.gov/us-eu-safe-harbor-framework (last accessed Mar. 6, 2014).
[51] Facebook, *Safe Harbor*, https://www.facebook.com/safeharbor.php (last accessed Mar. 6, 2014).

WhatsApp.[52] His investigation is focusing on the collection of data from WhatsApp users' address books and the potential for misuse of that information.[53]

44. Thilo Weichert, the data protection commissioner for the German state of Schleswig-Holstein, has also begun an investigation into the acquisition.[54] He told *Bloomberg*, "The mixing of data is strictly regulated by German law, especially through the Telemedia Act and the Federal Data Protection Act. Both acts rely on the principle of purpose binding, that data stored for one purpose cannot be processed for any other purposes - there are no such restrictions in the U.S."[55]

45. Commissioner Kohnstamm, who served as the head of the European Union's Article 29 Data Protection Working Party until February 27, 2014, said that any of the European Union's "28 data protection regulators could open an investigation" into the acquisition as well.[56]

IV. Legal Analysis

A. The FTC's Section 5 Authority

46. The FTC Act prohibits unfair and deceptive acts and practices, and empowers the Commission to enforce the Act's prohibitions.[57] These powers are described in FTC Policy Statements on Deception[58] and Unfairness.[59]

47. A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[60]

48. The injury must be "substantial."[61] Typically, this involves monetary harm, but may also include "unwarranted health and safety risks."[62] Emotional harm and

---

[52] Gibbs, *supra* at 47.
[53] *Id.*
[54] Jabeen Bhatti and Stephanie Bodoni, *Facebook Purchase of WhatsApp Raises German, Dutch, Art. 29 Privacy Concerns*, BLOOMBERG BNA, Mar. 3, 2014, http://www.bna.com/facebook-purchase-whatsapp-n17179882555.
[55] *Id.*
[56] Bodoni, *supra* at 46.
[57] *See* 15 U.S.C. § 45 (2010).
[58] Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm [hereinafter FTC Deception Policy].
[59] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), available at http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [hereinafter FTC Unfairness Policy].
[60] 15 U.S.C. § 45(n); *see, e.g.*, *Fed. Trade Comm'n v. Seismic Entertainment Productions, Inc.*, Civ. No. 1:04-CV- 00377 (Nov. 21, 2006) (finding that unauthorized changes to users' computers that affected the functionality of the computers as a result of Seismic's anti-spyware software constituted a "substantial injury without countervailing benefits.").
[61] FTC Unfairness Policy, *supra.*

other "more subjective types of harm" generally do not make a practice unfair.[63] Secondly, the injury "must not be outweighed by an offsetting consumer or competitive benefit that the sales practice also produces."[64] Thus the FTC will not find a practice unfair "unless it is injurious in its net effects."[65] Finally, "the injury must be one which consumers could not reasonably have avoided."[66] This factor is an effort to ensure that consumer decision making still governs the market by limiting the FTC to act in situations where seller behavior "unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."[67] Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence highly susceptible classes of consumers.[68]

49. An act or practice is deceptive if it involves a representation, omission, or practice that is likely to mislead the consumer acting reasonably under the circumstances, to the consumer's detriment."[69]

50. There are three elements to a deception claim. First, there must be a representation, omission, or practice that is likely to mislead the consumer.[70] The relevant inquiry for this factor is not whether the act or practice actually misled the consumer, but rather whether it is likely to mislead.[71]

51. Second, the act or practice must be considered from the perspective of a reasonable consumer.[72] "The test is whether the consumer's interpretation or reaction is reasonable."[73] The FTC will look at the totality of the act or practice and ask questions such as "how clear is the representation? How conspicuous is any qualifying information? How important is the omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?"[74]

---

[62] *Id.*; *see, e.g.*, *Fed. Trade Comm'n v. Information Search, Inc.*, Civ. No. 1:06-cv-01099 (Mar. 9, 2007) ("The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers' authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers.").
[63] FTC Unfairness Policy, *supra.*
[64] *Id*.
[65] *Id*.
[66] *Id*.
[67] *Id*.
[68] *Id*.
[69] FTC Deception Policy, *supra*.
[70] FTC Deception Policy, *supra* ; *see, e.g.*, *Fed Trade Comm'n v. Pantron I Corp.*, 33 F.3d 1088 (9th Cir. 1994) (holding that Pantron's representation to consumers that a product was effective at reducing hair loss was materially misleading, because according to studies, the success of the product could only be attributed to a placebo effect, rather than on scientific grounds).
[71] FTC Deception Policy, *supra*.
[72] *Id.*
[73] *Id.*
[74] *Id.*

52. Finally, the representation, omission, or practice must be material.[75] Essentially, the information must be important to consumers. The relevant question is whether consumers would have chosen another product if the deception had not occurred.[76] Express claims will be presumed material.[77] Materiality is presumed for claims and omissions involving "health, safety, or other areas with which the reasonable consumer would be concerned."[78]

53. The FTC presumes that an omission is material where "the seller knew, or should have known, that an ordinary consumer would need omitted information to evaluate the product or service, or that the claim was false . . . because the manufacturer intended the information or omission to have an effect."[79]

54. The Commission has previously found that a company may not alter the privacy settings of its users.[80]

55. The Commission has previously found that a company may not repurpose user data for a use other than the one for which the user's data was collected without first obtaining the user's "express affirmative consent."[81]

56. In the FTC's consideration of the Google acquisition of Doubleclick, where similar issues were raised about the impact on user privacy, the Commission allowed the merger to go forward, but only because the Commission found that the scope of its antitrust review did not encompass issues related to consumer privacy.[82]

57. In the Google acquisition of Doubleclick, Commissioner Harbor dissented and warned, "The truth is, we really do not know what Google/DoubleClick can or will do with its trove of information about consumers' Internet habits. The merger creates a firm with vast knowledge of consumer preferences, subject to very little accountability."[83]

---

[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 110 (1984).
[80] *In the Matter of Facebook, Inc., a corporation; FTC File No. 092 3184*, FTC.gov (Dec. 30, 2011), http://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.
[81] *In the Matter of Google, Inc.;* FTC File No. 102 3136 (Oct. 13, 2011) (Decision and Order), http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.
[82] *In the Matter of DoubleClick, Inc.*, FTC File No. 071-0170 (2000) (Statement of the Commission), http://www.ftc.gov/sites/default/files/documents/cases/2007/12/071220statement.pdf.
[83] *In the Matter of DoubleClick, Inc.*, FTC File No. 071-0170 (2000) (Dissenting Statement of Commissioner Pamela Jones Harbour), http://www.ftc.gov/os/caselist/0710170/071220harbour.pdf.

B. Count I: Deceptive Failure to Represent that WhatsApp's Governing Principles of Anonymity and Privacy Were Subject to Reversal

58. As described above, WhatsApp represented to consumers that the company will not retain or repurpose information collected from their mobile phones.

59. As described in detail above, facts about WhatsApp's philosophy of privacy and anonymity were material to users in their decision to install and use WhatsApp.

60. As described above, some users selected WhatsApp as a pro-privacy alternative to other messaging services.

61. Therefore, WhatsApp's failure to adequately disclose that this commitment to privacy was subject to reversal constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

62. Users could not reasonably avoid being aware of the inadequate disclosures regarding the potential for reversal of the privacy policy.

63. The inadequate disclosures are not outweighed by countervailing benefits to consumers or to competition.

64. WhatsApp's inadequate disclosures constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

C. Count II: Unfair Failure to Adequately Protect User Data In the Event of an Acquisition

65. As described in detail above, WhatsApp users reasonably expected that selecting WhatsApp would provide them with a privacy-protective messaging service.

66. As described in detail above, industry experts have identified that Facebook's acquisition of WhatsApp will dramatically expand Facebook's ability to gather user data.

67. As described in detail above, Facebook regularly collects and stores virtually all user information that it can extract.

68. By failing to make special provisions to protect user data in the event of an acquisition, WhatsApp "unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."

69. Specifically, WhatsApp users could not reasonably have anticipated that by selecting a pro-privacy messaging service, they would subject their data to Facebook's data collection practices.

70. The inadequate protections are not outweighed by countervailing benefits to consumers or to competition.

71. Therefore, WhatsApp's inadequate disclosures constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(n).

V. Prayer for Investigation and Relief

1. EPIC urges the Commission to investigate WhatsApp, Inc., and enjoin its unfair and deceptive data collection practices for any future changes to its privacy policy.

2. Specifically, EPIC requests the Commission to:

    a. Initiate an investigation of the proposed acquisition of WhatsApp by Facebook specifically with regard to the ability of Facebook to access WhatsApp's store of user mobile phone numbers and metadata;

    b. Until the issues identified in this Complaint are adequately resolved, use the Commission's authority to review mergers to halt Facebook's proposed acquisition of WhatsApp;

    c. In the event that the acquisition proceeds, order Facebook to insulate WhatsApp users' information from access by Facebook's data collection practices; and

    d. Provide such other relief as the Commission finds necessary and appropriate.

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director
Julia Horwitz, EPIC Consumer Protection Counsel
Ginger McCall, EPIC Associate Director
Khaliah Barnes, EPIC Administrative Law Counsel
Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)

Jeff Chester, CDD Executive Director
Hudson Kingston, CDD Legal Director
Center for Digital Democracy
1621 Connecticut Ave. NW Suite 550
Washington, DC 20009
(202) 332-2670 (tel)